

ServerView Suite Enterprise Edition V2.41

Installationshandbuch

Ausgabe Mai 2009

Kritik... Anregungen... Korrekturen...

Die Redaktion ist interessiert an Ihren Kommentaren zu diesem Handbuch. Ihre Rückmeldungen helfen uns, die Dokumentation zu optimieren und auf Ihre Wünsche und Bedürfnisse abzustimmen.

Sie können uns Ihre Kommentare per E-Mail an manuals@ts.fujitsu.com senden.

Zertifizierte Dokumentation nach DIN EN ISO 9001:2000

Um eine gleichbleibend hohe Qualität und Anwenderfreundlichkeit zu gewährleisten, wurde diese Dokumentation nach den Vorgaben eines Qualitätsmanagementsystems erstellt, welches die Forderungen der DIN EN ISO 9001:2000 erfüllt.

cognitas. Gesellschaft für Technik-Dokumentation mbH
www.cognitas.de

Copyright und Handelsmarken

Copyright © Fujitsu Technology Solutions GmbH 2009.

Alle Rechte vorbehalten.

Liefermöglichkeiten und technische Änderungen vorbehalten.

Alle verwendeten Hard- und Softwarenamen sind Handelsnamen und/oder Warenzeichen der jeweiligen Hersteller.

Inhaltsverzeichnis

1	Einleitung	7
1.1	Zielgruppen	7
1.2	Darstellungsmittel	8
2	Übersicht	9
2.1	Architektur	9
2.2	Verwaltungsschritte	9
3	Management-Server	13
3.1	Voraussetzungen	13
3.2	Installation	16
3.3	Deinstallation	16
3.4	Konfiguration	17
3.4.1	Hardware-Überwachung	17
3.4.2	Administrationsfunktionen	18
3.4.3	Life Cycle Management	18
3.5	Fehlerbehebung	19
4	Verwaltungsarbeitsplatz	23
4.1	Voraussetzungen	24
4.1.1	Verwaltungsarbeitsplatz mit Windows	24
4.1.2	Verwaltungsarbeitsplatz mit Linux	24
4.2	Installation	25
4.2.1	Installation auf Windows-Systemen	25
4.2.1.1	Lokale Java-Anwendung	25
4.2.1.2	Java Web Start-Anwendung	26
4.2.2	Installation auf Linux-Systemen	26

Inhaltsverzeichnis

4.3	Deinstallation	27
4.3.1	Deinstallation auf Windows-Systemen	27
4.3.2	Deinstallation auf Linux-Systemen	27
4.4	Konfiguration	27
5	Verwaltete Knoten	29
5.1	Voraussetzungen	29
5.1.1	PRIMERGY-Server mit Windows	29
5.1.2	PRIMERGY-Server mit Linux	29
5.1.3	PRIMEQUEST-Partitionen mit Windows	30
5.1.4	PRIMEQUEST-Partition mit Linux	30
5.1.5	PRIMEPOWER mit Solaris	31
5.1.6	SPARC Enterprise Server mit Solaris	32
5.2	Installation	32
5.2.1	Installation auf PRIMEQUEST-Partitionen mit Windows	32
5.2.2	Installation auf PRIMERGY / PRIMEQUEST-Partitionen mit Linux	34
5.2.3	Installation auf PRIMEPOWER / SPARC ES-Partitionen	35
5.2.3.1	“LiveUpgrade“-Installation des Solaris ServerView Agenten	36
5.3	Deinstallation	37
5.3.1	Deinstallation auf Windows-Systemen	37
5.3.2	Deinstallation auf Linux-Systemen	37
5.3.3	Deinstallation auf Solaris-Systemen	37
5.4	Konfiguration	38
6	SNMP-Konfiguration	39
6.1	SNMP-Konfiguration auf dem Management-Server	40
6.2	SNMP-Konfiguration auf den verwalteten Knoten	41
6.2.1	Linux-System	41
6.2.1.1	Konfiguration des SNMP-Master-Agenten	42
6.2.1.2	Konfiguration der SNMP-ServerView-Agenten	44
6.2.1.3	Starten und Stoppen der SNMP-Agenten	44
6.2.2	Windows-System	45
6.2.2.1	SNMP-Dienst installieren und aktivieren	46
6.2.2.2	SNMP-ServerView-Agenten aktivieren	47

7	Kommunikationswege absichern	49
7.1	SSL für TCP/IP-Verbindungen	49
7.1.1	Aufbau einer sicheren Domäne	50
7.1.2	Aufbau eines selbstsignierten Benutzerzertifikats	51
7.1.2.1	Verwendung von MK_KEY	51
7.1.2.2	Verwendung der openssl-Kommandos	51
7.1.3	Installation von öffentlichen und privaten Schlüsseln	53
7.1.4	Anmeldeverfahren	55
7.1.5	Fehlersituationen	56
7.2	Kommunikation mittels HTTPS absichern	57
8	Portkonfiguration	59
8.1	Fest zugewiesene Ports	59
8.1.1	Fest zugewiesene Ports auf dem Management-Server	59
8.1.2	Fest zugewiesene Ports auf den verwalteten Knoten	60
8.1.2.1	Windows-System: PRIMERGY- und PRIMEQUEST-Systeme	60
8.1.2.2	Linux-System	60
8.1.2.3	Solaris-Systeme	60
8.1.2.4	MMB	61
8.1.2.5	XSCF	61
8.1.3	Rekonfigurierung von Port 8886: WSAServer	61
8.1.4	Rekonfigurierung von Port 8899: dom_adm	62
8.1.5	Rekonfigurierung der Ports 8881-8883: Webserver-Ports	62
8.2	Dynamisch zugewiesene Ports	63
8.2.1	Dynamisch zugewiesene Ports auf dem Verwaltungsarbeitsplatz	63
8.2.2	Dynamisch zugewiesene Ports auf dem Management-Server	65
8.2.3	Rekonfigurierung dynamisch zugewiesener Ports	67
9	PRIMEQUEST konfigurieren	69
9.1	Einstellungen im MMB-Web UI	69
9.1.1	Verwaltungs-LAN konfigurieren	69
9.1.2	SNMP aktivieren	71
9.1.3	SNMP konfigurieren	73
9.1.3.1	SNMP-Protokollparameter	73
9.1.3.2	SNMP-Trap-Parameter	75

Inhaltsverzeichnis

9.1.4	Access Control konfigurieren	77
9.1.5	Remote Server Management konfigurieren	78
9.2	IP-Adresse des MMB ändern	80
9.3	Konfiguration der Partition ändern	80
9.4	Aktualisieren von Management-Server-Einstellungen	81
10	SPARC ES konfigurieren	83
10.1	Öffentlicher SSH-Schlüssel des XSCF-Boards	83
10.2	Öffentlicher SSH-Schlüssel auf dem verwalteten Knoten	85
10.3	Konfigurationsänderungen	85
10.3.1	Öffentlichen SSH-Schlüssel auf dem Management-Server ändern	86
10.3.2	Öffentlichen SSH-Schlüssel oder IP-Adresse des XSCF-Boards ändern	87
10.3.3	Öffentlichen SSH-Schlüssel, Hostname oder IP-Adresse des verwalteten Knotens ändern	87
10.3.4	Portnummer für die SSH-Kommunikation ändern	89
10.3.5	Agent mit bereits registrierter SSH-Information	90
11	Anhang	91
11.1	Konfiguration der SV-SNMP-Agenten unter Linux	91
11.2	Konfiguration der SV-SNMP-Agenten unter Windows	93
	Abkürzungen	97
	Stichwörter	99

1 Einleitung

Die *ServerView Suite Enterprise Edition* vereinigt verschiedene System-Management-Oberflächen unterschiedlicher Server-Familien (PRIMEQUEST, PRIMERGY, PRIMEPOWER, SPARC Enterprise Server) unter einer einzigen Oberfläche. Das vorliegende Handbuch beschreibt die Installation und Konfiguration der *ServerView Suite Enterprise Edition* (im Folgenden kurz *ServerView Suite* bzw. *SVS EE* genannt).



Dieses Produkt war früher als *WebSysAdmin* (abgekürzt WSA) bekannt. Die Abkürzung WSA ist noch häufig in Pfaden und Dateinamen zu finden.

1.1 Zielgruppen

Dieses Handbuch wendet sich an Systemverwalter und Mitarbeiter des Kundendienstes. Vorausgesetzt werden gute Betriebssystem- und Hardware-Kenntnisse.

1.2 Darstellungsmittel

In diesem Handbuch werden folgende Darstellungsmittel verwendet:

kursive Schrift

Namen von Kommandos, Systemaufrufen, Funktionen, Dateien, Prozeduren, Programmen usw. sowie Menüeinträge und Ein-/Ausgabefelder von Abbildungen im Fließtext

Name(Extension)

Kommandos, Systemaufrufe, Funktionen, Dateien, Schnittstellen usw., zu denen Manual-Pages (Beschreibungen) vorliegen, sind mit einer in Klammern angegebenen Extension versehen. Die Extension bezeichnet das Kapitel, in dem die Manual-Page beschrieben ist.

Manual-Pages können Sie sich auf dem Bildschirm mit dem Kommando *man* [siehe *man(1)*] anzeigen lassen. Hinweise zur Benutzung dieses Kommandos erhalten Sie, wenn Sie sich die Manual-Page zum *man*-Kommando selbst anzeigen lassen. Geben Sie dazu *man man* ein.

dicktengleiche Schrift

Systemausgaben wie Fehlermeldungen, Nachrichten, Hinweise, Dateiauszüge und Programmbeispiele

dicktengleiche halbfette Schrift

Benutzereingaben in Beispielen

► Aktivitäten des Benutzers



Zusätzliche Hinweise, die zum Verständnis der umgebenden Textpassagen beachtet werden sollten.

2 Übersicht

2.1 Architektur

Die Architektur der *ServerView Suite* kann in drei Bereiche aufgeteilt werden, wie in der folgenden Grafik von links nach rechts dargestellt:

1. Verwaltungsarbeitsplatz (PC-Client bzw. Frontend)
2. Management-Server (MS)
3. verwaltete Knoten

Alle genannten drei Komponenten müssen bestimmte Voraussetzungen erfüllen und verwaltet werden.

In den nächsten Kapiteln werden alle notwendigen Verwaltungsschritte beschrieben.

2.2 Verwaltungsschritte

Insgesamt sind folgende Verwaltungsschritte notwendig:

- SW- und HW-Voraussetzungen schaffen
- Installation bzw. Deinstallation
- Konfiguration

Entsprechend der Architektur der *ServerView Suite* sind bestimmte Software- und Hardware-Voraussetzungen zu berücksichtigen, und zwar für:

- den Verwaltungsarbeitsplatz
- den Management-Server (MS)
- die verwalteten Knoten

Desgleichen sind bei der Installation bzw. der Deinstallation der *ServerView Suite* wieder die drei Bereiche zu unterscheiden:

- Installation und Deinstallation auf dem Verwaltungsarbeitsplatz
- Installation und Deinstallation auf dem Management-Server (MS)
- Installation und Deinstallation auf den verwalteten Knoten: PRIMEPOWER (PW), PRIMERGY (PY), SPARC Enterprise Server (SPARC ES) und PRIMEQUEST (PQ-Part.)

Konfigurationsanpassungen müssen auf dem Management-Server und den verwalteten Knoten vorgenommen werden für:

- die SNMP-Kommunikation
- die Kommunikation mit dem MMB der PRIMEQUEST
- die Kommunikation mit dem XSCF und den Partitionen eines SPARC Enterprise Servers

Die folgende Übersicht veranschaulicht die gesamte Architektur mit allen Netzwerkverbindungen.

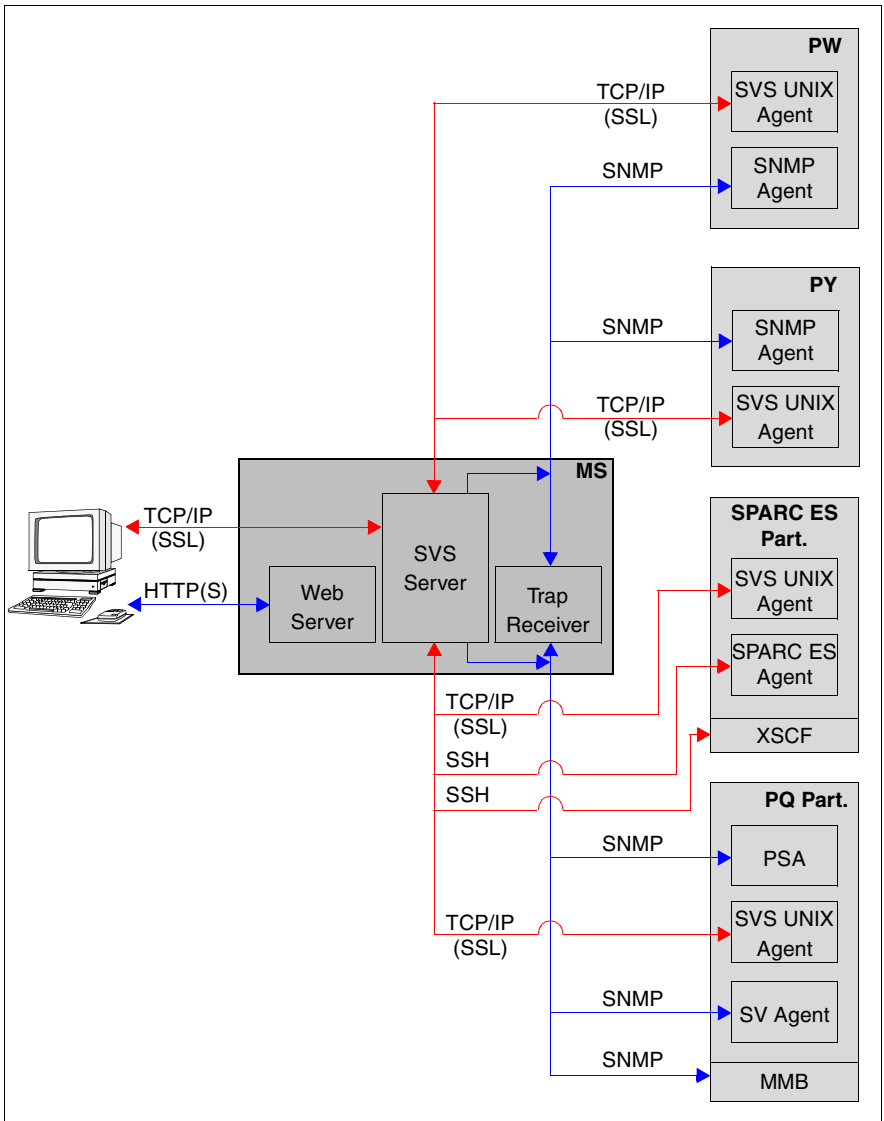


Bild 1: ServerView Suite-Architektur

3 Management-Server

3.1 Voraussetzungen

Der Manager-Teil der *ServerView Suite* kann auf jedem beliebigen Linux-System installiert werden, das folgende Voraussetzungen erfüllt:

- x86-System (PRIMERGY empfohlen) mit mindestens
 - 1 GB Speicher (2 GB empfohlen)
 - 2 GHz CPU
 - 500 MB freiem Plattenspeicherplatz
 - 17" Bildschirm mit XGA-Auflösung
- Als Betriebssystem wird vorausgesetzt:
 - SLES9 SP3 (nur die x86-Variante)
 - SLES10 SP1 (nur die x86-Variante)
 - SLES10 SP2 (x86-, Intel64- oder AMD64-Variante)
 - RHEL 5.1 (nur die x86-Variante)
 - RHEL 5.2 (x86-, Intel64- oder AMD64-Variante)
 - RHEL 5.3 (x86-, Intel64- oder AMD64-Variante)
- Folgende Pakete müssen installiert sein:
 - *apache2* (SLES) oder *httpd* (RHEL)
 - *at*
 - *net-snmp* Version 5.1.3.1-0.6 oder höher (SLES)
 - *net-snmp* Version 5.1.2-11.EL4.6 oder höher (RHEL)
 - *net-snmp-utils* (RHEL)
 - *openssl*
 - *perl*
 - *zlib*
 - *inetd* or *xinetd*
 - *unixODBC* Version 2.2.11 oder höher
 - *unixODBC-devel* (RHEL)
 - *expect*
 - *compat-2004* (SLES9)
 - *compat-2006.1.25-11.2* und *compat-libstdc++-5.0.7-22.2* (SLES10)
 - *compat-libstdc++-296* und *compat-libstdc++-33-3.2.3-47.3* oder höher (RHEL)
 - *openssh* (SLES) oder *openssh-clients* (RHEL)
 - *libX11* (RHEL 5.1 oder höher)

- *libXp* (RHEL 5.1 oder höher)
- *bash*

Besondere Anforderungen für Intel64-/AMD64-Varianten:

- *unixODBC* ist für beide Varianten x86(i386) und Intel64/AMD64(x86_64) erforderlich
- *unixODBC-devel* ist nur für die x86(i386)-Variante erforderlich (RHEL)
- *net-snmp-libs* ist für beide Varianten x86(i386) und Intel64/AMD64(x86_64) erforderlich (RHEL)
- Upgrade des Kernels 2.6.16.60-0.23 (Linux-Kernel 20080515) oder höher:

Wegen eines Problems im *netstat*-Kommando müssen alle aktuell installierten Kernel-Pakete ersetzt werden (SLES10 SP2 Intel64-/AMD64-Variante(x86_64)).

i Beachten Sie bitte, dass der Service *atd*, der Web-Service (*apache2* (SLES) oder *httpd* (RHEL)) und einer der Services *inetd* oder *xinetd* aktiviert sein müssen. Diese Dienste können Sie über die Kommandozeilenebene mit dem Kommando *chkconfig* aktivieren (siehe *man chkconfig*) oder über die jeweils installierte Systemverwaltungsapplikation:

- Auf SLES mit *YaST2*
Wählen Sie im Menü *System* → *Runlevel Editor*
 - Auf RHEL mit *Serviceconf*
- Stellen Sie sicher, dass die Datei */etc/hosts* einen Eintrag mit der öffentliche IP-Adresse des Management-Servers und seinem Hostnamen enthält.

Darüber hinaus ist es erforderlich, dass in der Datei */etc/hosts* die IP-Adresse 127.0.0.1 (*localhost*) enthalten ist. Sie ist für den Zugriff auf den PostgreSQL-Server erforderlich.

Beispiel für diese beiden Zeilen in der Datei */etc/hosts*:

```
<IP address> <full qualified host name> <short host name>
127.0.0.1      localhost.localdomain    localhost
```

- Stellen Sie sicher, dass Zeitzone und Systemzeit auf die lokale Zeit des Standortes eingestellt sind, an dem der Server betrieben wird (siehe *man hwclock*).

- Bei RHEL 5.1 oder höher muss SELinux deaktiviert sein. Sie erreichen dies, indem Sie in der Datei `/etc/sysconfig/selinux` die entsprechende Zeile (`SELINUX=`) wie folgt ändern:

`SELINUX=disabled`

Anschließend muss das System neu gestartet werden. Weitere Informationen über SELinux finden Sie unter <http://www.ittvis.com/services/tech-tip.asp?tid=3092>

- Bei SLES10 SP1 und RHEL 5.1 oder höher ist der SNMP-Trapempfang standardmäßig deaktiviert. Sie aktivieren den Trapempfang, indem Sie die folgende Zeile in `/usr/share/snmp/snmptrapd.conf` hinzufügen:

`disableAuthorization yes`

Falls Sie die *ServerView Suite* bereits installiert haben, muss nach einer Änderung von `snmptrapd.conf` der `trpsrvd`-Dienst neu gestartet werden.

Rufen Sie hierfür auf:

```
# /etc/init.d/WsaSnmp stop
# /etc/init.d/trpsrvd stop
# /etc/init.d/trpsrvd start
# /etc/init.d/WsaSnmp start
```

Weitere Informationen über Trapempfang finden Sie unter <http://net-snmp.sourceforge.net/docs/man/snmptrapd.conf.html>

- Überprüfen Sie zunächst die folgenden Punkte, bevor Sie das Installations-script ausführen:
 - Die Spracheinstellung darf nicht mit „C“ oder „“ vorgenommen werden, weil die Installation der Postgre-Datenbasis dies nicht unterstützt und die Installation hierdurch an irgendeinem Punkt fehlschlägt. Verwenden Sie für die Spracheinstellung einen richtigen Wert vor (z. B. „en_US.UTF-8“).
 - Wenn ein Update sowohl für *ServerView Suite* als auch für das Betriebssystem erforderlich ist, muss der Update des Betriebssystems zuerst vorgenommen werden.



Bevor Sie eine Update-Installation durchführen können, müssen alle SVS EE-Sitzungen auf den Verwaltungsarbeitsplätzen geschlossen werden (dies wird vom *installer*-Skript überprüft).

Eine Update-Installation berücksichtigt automatisch alle SVS EE Versionen V1.0 oder höher.

3.2 Installation

Die *ServerView Suite* wird installiert, indem das Skript *installer*, das sich im Verzeichnis *ServerView_Suite_Enterprise_Edition* befindet, ausgeführt wird.

Gehen Sie dazu wie folgt vor:

- ▶ Hängen Sie das ISO-Image in ein existierendes Verzeichnis ein, z. B. in */media*:

```
# mount -o loop <absolute_pathname_of_the_ISO_file> /media
```
- ▶ Wechseln Sie in das Verzeichnis des zu installierenden Produkts:

```
# cd /media/ServerView_Suite_Enterprise_Edition
```
- ▶ Starten Sie die Installation durch folgendes Kommando:

```
# ./installer
```

Ein Text wie der folgende erscheint:

```
+++ Installation of ServerView Suite Enterprise Edition started.
```

Folgen Sie den angezeigten Anweisungen.



Falls bei der Installation des Paketes *ServerViewStarter* irgendwelche Probleme auftreten, geben Sie bitte im Verzeichnis *ServerView Suite Enterprise Edition/all* das Kommando *InstallServerView -upgrade* ein.

- ▶ Wenn die Installation beendet ist, verlassen Sie das Einhänge-Verzeichnis und hängen Sie es aus, z. B.:

```
# cd /  
# umount /media
```

3.3 Deinstallation

Wenn der Management-Server deinstalliert werden soll, sollten Sie zuerst die Domäne entfernen. Starten Sie das GUI und löschen Sie alle Knoten aus der Domäne. Entfernen Sie anschließend den Management-Server.

Die *ServerView Suite* wird deinstalliert durch Aufruf von */opt/SMAW/deinstaller.ServerView_Suite_Enterprise_Edition*.



Bevor Sie die Software deinstallieren können, müssen alle SVS EE-Sitzungen auf den Verwaltungsarbeitsplätzen geschlossen werden (dies wird vom *deinstaller*-Skript überprüft).

3.4 Konfiguration



Das Passwort des Domänen-Verwalters *wdmadm* ist voreingestellt! Es wird empfohlen, das Passwort auf allen Systemen zu ändern (siehe 5.1.2 *Ändern des Passwortes für den Domänen-Verwalter „wdmadm“* im aktuellen *ServerView Suite EE Benutzerhandbuch Rechnerverwaltung in einer Domäne*) oder - noch besser - SSL-Verschlüsselung zu verwenden. Einzelheiten zur SSL-Konfigurierung finden Sie in [Abschnitt „SSL für TCP/IP-Verbindungen“ auf Seite 49](#).

Die *ServerView Suite* kommuniziert mit den verwalteten Knoten über TCP/IP und SNMP. Hierzu werden Ports auf dem Management-Server und den verwalteten Knoten belegt.

Informationen zur SNMP-Konfiguration finden Sie im [Abschnitt „SNMP-Konfiguration auf dem Management-Server“ auf Seite 40](#).

Die Standardbelegung der fest zugewiesenen Ports und die Bereiche für die dynamisch zugewiesenen Ports können geändert werden. Nähere Informationen finden Sie im [Kapitel „Portkonfiguration“ auf Seite 59](#).

Nähere Informationen zur Konfiguration von SPARC Enterprise-Systemen finden Sie im [Kapitel „SPARC ES konfigurieren“ auf Seite 83](#).

Wollen Sie mit der SVS EE eine sichere, auf SSL basierende Verwaltungsdomäne aufbauen, so müssen Sie auf dem Management-Server für jeden SVS EE-Benutzer eine Benutzerkennung anlegen und seinen privaten und öffentlichen Schlüssel installieren. Nähere Informationen finden Sie im [Kapitel „Kommunikationswege absichern“ auf Seite 49](#).

3.4.1 Hardware-Überwachung

Die Hardware-Überwachung erfolgt für PRIMEQUEST-Systeme ohne SVS-Komponenten auf den überwachten Knoten und auf allen Betriebssysteme.



Für PRIMERGY-, PRIMEPOWER- und SPARC Enterprise-Systeme ist der jeweils geeignete ServerView Agent erforderlich.

3.4.2 Administrationsfunktionen

Die aktuelle Software-Version von SVS EE unterstützt unter anderem die folgenden Administrationsfunktionen:

- Benutzerverwaltung und Benutzergruppenverwaltung
- Cron-Job-Administration für den Benutzer *root*
- Anzeige, Überprüfung und Löschen von Software-Paketen
- Auswertung und Konfigurierung von Log-Dateien
- Prozessmanagement (Anzeige / Löschen von Prozessen)
- Dateisystem- und NFS-Administration (nur für Solaris)



Für die Systemverwaltungsfunktionen muss auf jedem Knoten, der administriert werden soll, das Produkt ServerView Suite Enterprise Edition Agent installiert sein. Gegenwärtig werden nur Linux und Solaris unterstützt.

3.4.3 Life Cycle Management

Life Cycle Management beinhaltet Asset und Performance Management für PRIMERGY- und PRIMEQUEST-Systeme. Um diese Funktionen nutzen zu können, muss der jeweils geeignete auf den zu überwachenden Knoten installiert sein.



Bitte beachten Sie, dass es wegen interner Update-Mechanismen auf PRIMEQUEST-Systemen nach Konfigurationsänderungen möglicherweise fast 30 Minuten dauern kann, bis die neuen Daten zur Verfügung stehen. Die Ergebnisse von DP-Aktionen (Dynamic Partitioning) sind überdies in der grafischen Bedienoberfläche des Performance Managers erst nach einem Neustart des Betriebssystems sichtbar.

3.5 Fehlerbehebung

- Bei Auftreten der Problemmeldung „Open UDP connection to server failed! Please check your server configuration. Try again?“ überprüfen Sie bitte die *inetd*- oder *xinetd*-Konfiguration.



Beachten Sie bitte, dass der Service *atd*, der Web-Service (*apache2* (SLES) oder *httpd* (RHEL)) und einer der Services *inetd* oder *xinetd* aktiviert sein müssen. Diese Dienste können Sie über die Kommandozeilenebene mit dem Kommando *chkconfig* aktivieren (siehe *man chkconfig*) oder über die jeweils installierte Systemverwaltungsapplikation:

- Auf SLES mit *YaST2*
Wählen Sie im Menü *System* → *Runlevel Editor*
 - Auf RHEL mit *Serviceconf*
- Bei Auftreten der Problemmeldung „Cannot create PRIMEQUEST Server“ besteht wahrscheinlich die Ursache in einer inkompatiblen Einstellung von PRIMEQUEST MMB Web-UI und Management Server. Empfohlen ist folgendes Vorgehen:
 - Überprüfen Sie die SNMP/IPMI-Einstellungen des PRIMEQUEST MMB Web-UI erneut.
 - Überprüfen Sie die Zugangsberechtigungen im SVS EE GUI im Hinblick auf die Einstellungen im MMB.

Falls dieses Problem nicht gelöst werden kann, sichern Sie bitte die Log-Dateien im Verzeichnis */tmp/work* unter Verwendung folgender Kommandos:

```
# /bin/mkdir /tmp/work
# cd /
# /opt/FJSPqsc/sbin/pqsc_snap -d /tmp/work
# /bin/tar zcvf /tmp/work/SMAW_trace.tar.gz \
opt/SMAW/tmp/WSATrace
```

Schicken Sie die Log-Dateien */tmp/work/*tar.gz* zum Support von Fujitsu / Fujitsu Technology Solutions.

- Möglicherweise, jedoch sehr selten, kann es vorkommen, dass ein Server-View-Paket nicht deinstalliert werden kann. Sie können das folgende Kommando verwenden, um festzustellen, ob andere Pakete von dem Paket abhängig sind, das Sie deinstallieren wollen:

```
# rpm -q --whatrequires <package>
```

Falls abhängige Pakete existieren, deinstallieren Sie diese zuerst mit folgendem Kommando:

```
# rpm -e <package>
```

Falls Sie Fehlermeldungen erhalten, deinstallieren Sie die Pakete mit dem folgenden Kommando:

```
# rpm -e --noscripts <package>
```

Folgende Pakete sind installiert:

- *SMAWPbase*
- *SMAWPpgsq*
- *ServerViewDB*
- *ServerViewCommon*
- *AlarmService*
- *ServerView_S2*

Deinstallieren Sie die Pakete in umgekehrter Reihenfolge, beginnend mit *ServerView_S2*.

Falls *SMAWPbase* von anderen Paketen benötigt wird, deinstallieren Sie es nicht. Überprüfen Sie ebenfalls, ob ein Paket *ServerViewStarter* installiert ist, und falls dies der Fall ist, deinstallieren Sie es.

- Möglicherweise, jedoch sehr selten, kann es vorkommen, dass ein Installations- oder Deinstallationsprozess nicht korrekt durchläuft. Um das System von Life Cycle Modules zu reinigen, deinstallieren Sie zunächst alle abhängigen Pakete und dann die Pakete selbst.

Anschließend müssen Sie folgende Verzeichnisse löschen:

- *WebServerDocumentRoot>/ServerView*
- *<WebServerScripts>/ServerView*
- */opt/SMAWPlus/pgsql*
- */usr/bin/setServerViewEnviron**
- */usr/bin/setSVParams**
- */usr/bin/UninstallServerView**

- Wenn Sie ein ungewöhnliches Verhalten des GUI beobachten (insbesondere bei Anwahl von *Alarm Service* → *Server Settings* → *Filter Server*), hat sich möglicherweise mit JRE 1.6.0_10 oder höher die Plugin-Architektur geändert. Klicken Sie in diesem Fall auf den *Advance*-Reiter im Java Control Panel und deaktivieren Sie die Check Box *Enable the next-generation Java Plug-in*.

Weitere Problemlösungen finden Sie im aktuellen *ServerView Suite EE* Benutzerhandbuch *Rechnerverwaltung in einer Domäne*. Insbesondere bei Problemen mit Java Web Start finden Sie hier Hilfe im Abschnitt *3.2.3 Produkt mit Hilfe von Java Web Start starten*.

4 Verwaltungsarbeitsplatz

Der Verwaltungsarbeitsplatz kann auf einem Windows- oder einem Linux-System eingerichtet werden. Der Verwaltungsarbeitsplatz auf Linux muss zugleich der Management-Server sein.

Handbücher sowie Teile der zu installierenden Software können mit Hilfe eines Web-Browsers vom Management-Server (über die URL `<host>:8883`) heruntergeladen werden.

FUJITSU **ServerView® Suite** ENTERPRISE EDITION

Products for Download

Product	Version	Info
Windows Frontend, JRE, and Manuals (in PDF)		
Java™ 2 Runtime Environment	1.6.0_07	JRE 1.6.0 from SUN (Win32-International)
ServerView Suite Enterprise Edition (Windows Application) Readme.txt for installation	V 2.41	Win32 Java application (recommended) Please verify you have installed JRE >= 1.5.0_09 already!
Product Readme	V 2.41	English
User Manual	V 2.41	English / German
Installation Guide	V 2.41	English / German
Performance Manager Manual	V 2.20	English / German
Archive Manager Manual	V 2.20	English / German
Inventory Manager Manual	V 2.20	English / German
Start As Remote Application Using Java™Web Start		
ServerView Suite Enterprise Edition (Java WebStart Application) Readme.txt for trouble shooting	V 2.41	Remote GUI Please verify you have installed a JRE >= 1.5.0_09 already!
ServerView Suite Enterprise Edition (Java Web Start Application, read-only mode)	V 2.41	The read-only version of the Web Start GUI. For further information please refer to Readme.txt
Java Policy Template		For further information please refer to Readme.txt

© Fujitsu Technology Solutions 2009

Powered by **JAVA** **APACHE**

Bild 2: Download-Seite auf dem Management-Server

4.1 Voraussetzungen

4.1.1 Verwaltungsarbeitsplatz mit Windows

Es muss ein x86-System mit mindestens folgenden Parametern vorhanden sein:

- 512 MB Speicher
- Pentium® III oder höher
- 200 MB verfügbarer Plattenplatz
- 17"-Display mit X VGA-Auflösung (empfohlen)
- Windows XP

Es muss ein Java Runtime Environment (JRE) installiert sein. Erforderlich ist JRE Version 1.5.0_09 oder höher. Ein aktuell unterstütztes JRE kann über die Downloadseite des Managementsservers (URL: `http://<host>:8883`) heruntergeladen werden.

Da einige der SVS EE-Benutzeroberflächen Web-basiert sind, muss auch einer der folgenden Webbrowser vorhanden sein:

- Internet Explorer 6 oder 7
- Mozilla Firefox 2.0

4.1.2 Verwaltungsarbeitsplatz mit Linux

Der Linux-Verwaltungsarbeitsplatz kann nur auf einem Linux-Management-Server eingerichtet werden, d. h. der Verwaltungsarbeitsplatz muss die unter [Abschnitt „Voraussetzungen“ auf Seite 13](#) genannten Voraussetzungen erfüllen.

Da einige der SVS EE-Benutzeroberflächen Web-basiert sind, muss als Webbrowser Mozilla Firefox 2.0 mit JRE-Plugin $\geq 1.5.0\_09$ installiert sein.



Um das Skript *svsee* ausführen zu können, müssen die Installationspakete *libX11-1.0.3-8.0.1.el5* und *libXp-1.0.0-8.1.el5* vorhanden sein.

4.2 Installation

4.2.1 Installation auf Windows-Systemen

Die Bedieneroberfläche von SVS EE kann auf einem Windows-System lokal als Java-Applikation oder über einen Browser als Java Web Start-Anwendung gestartet werden. Es wird empfohlen, die lokale Java-Anwendung zu benutzen.

4.2.1.1 Lokale Java-Anwendung

Wenn Sie mit *ServerView Suite* als lokaler Anwendung unter Windows arbeiten wollen, müssen Sie die Software von einem SVS EE-Management-Server herunterladen. Geben Sie dazu in der URL-Zeile des Browsers folgendes ein:

`http://<host>:8883`

z.B.: `http://discover-scm.pdb.fsc.net:8883`

Sie gelangen auf die Download-Seite von *ServerView Suite* und können das Produkt dort auswählen. Nachdem Sie das Produkt heruntergeladen haben, können Sie es wie jede andere Windows-Anwendung installieren.

Die Anwendung wird im Start-Menü unter *Programme* installiert. Von dort aus können Sie *ServerView Suite* lokal auf Ihrem PC starten.

Standardeinstellung für den Installationspfad ist:

`C:\<program_directory>\Fujitsu\WebSysAdmin\`



Wenn die JAVA-Laufzeitumgebung JRE auf dem Verwaltungsarbeitsplatz nach der *ServerView Suite*-Installation aktualisiert wurde, muss die *ServerView Suite*-Konfiguration entsprechend angepasst werden. Gehen Sie folgendermaßen vor:

- Reinstallieren Sie die *ServerView Suite* (empfohlenes Vorgehen)
oder
- Aktualisieren Sie mittels eines Editors den JRE-Pfadnamen in
`<installation_directory>\wsa.bat`

4.2.1.2 Java Web Start-Anwendung

Wenn Sie mit ServerView Suite als Java Web Start-Anwendung unter Windows arbeiten wollen, ist **keine** Installation auf dem Verwaltungsarbeitsplatz notwendig.

Aufruf:

Geben Sie eine der folgenden URLs im Webbrowser ein:

- `http://<host>:8881`
- `http://<host>:8882`
- `http://<host>:8883`

Über Port 8881 erhalten Sie einen Lese/Schreibzugriff über Port 8882 einen Nur-Lese-Zugriff (siehe auch [Kapitel „Portkonfiguration“ auf Seite 59](#)).

Bei Anwahl von Port 8883 wird die Downloadseite der *ServerView Suite* angezeigt. Wählen Sie hier den unter der Überschrift

Start As Remote Application Using Java™ Web Start aufgeführten Eintrag:

ServerView Suite Enterprise Edition
(Java Web Start Application)

Oder den Eintrag:

ServerView Suite Enterprise Edition
(Java Web Start Application, read-only mode)

4.2.2 Installation auf Linux-Systemen

Die Bedieneroberfläche der SVS EE kann auf einem Linux-System nur lokal als Java-Applikation gestartet werden.

Das GUI ist Teil der ServerView Suite Enterprise Edition für den Management-Server und wird automatisch mit installiert. Das GUI benutzt eine interne JRE (unter `/opt/SMAW/JavaForWsa` installiert).

Aufruf:

```
# /opt/SMAW/bin/svsee <hostname> &
```

4.3 Deinstallation

4.3.1 Deinstallation auf Windows-Systemen

Rufen Sie unter *Start – Programme – ServerView Suite Enterprise Edition* den Menüeintrag *Uninstall ServerView Suite Enterprise Edition* auf, um das Produkt zu deinstallieren.

4.3.2 Deinstallation auf Linux-Systemen

In diesem Fall muss nichts getan werden, da das GUI gelöscht wird, wenn der Management-Server deinstalliert wird.

4.4 Konfiguration

Wollen Sie die Bedieneroberfläche von SVS EE als sichere JAVA-Anwendung starten, so müssen Sie auf dem Verwaltungsarbeitsplatz

- das SSL-Protokoll konfigurieren
- die Benutzung des HTTPS-Protokolls aktivieren

Für das SSL-Protokoll müssen Sie Ihren privaten Schlüssel in der folgenden systemspezifischen Datei ablegen:

- Windows:

```
C:\wsa_certs\<login-username>\wsa_cert.p12
```

- Linux:

```
/opt/SMW/wsa_certs/<login_username>/wsa_cert.p12
```

Das HTTPS-Protokoll wird von den Life Cycle Modules (*Asset, Inventory, Performance, Update*) zur Kommunikation mit dem Management-Server verwendet. Die Aktivierung des HTTPS-Protokolls wird im [Abschnitt „Kommunikation mittels HTTPS absichern“ auf Seite 57](#) beschrieben.

Nähere Informationen zur SSL-Konfiguration finden Sie im [Abschnitt „SSL für TCP/IP-Verbindungen“ auf Seite 49](#).

5 Verwaltete Knoten

Es können folgende Hardware-Plattformen durch die SVS EE verwaltet werden:

- PRIMERGY (Linux- oder Windows-System)
- PRIMEPOWER (Solaris-System)
- PRIMEQUEST-Partition (Linux- oder Windows-System)
- SPARC Enterprise Server (Solaris-System)

5.1 Voraussetzungen

5.1.1 PRIMERGY-Server mit Windows

Auf PRIMERGY-Servern muss der ServerView-Agent von der neuesten Server-Start-DVD installiert sein.

Eine genaue Beschreibung des Installationsvorgangs finden Sie im Handbuch *PRIMERGY ServerView Suite; Installation; ServerView V4.61*.

5.1.2 PRIMERGY-Server mit Linux

Die folgenden Pakete müssen installiert sein:

- *at*
- *inetd* oder *xinetd*
- *openssl* (32-Bit-Version)
- *ServerView Agent* (von der ServerStart-DVD)
- *bash*
- *net-snmp* (Net-SNMP) Version 5.1.3.1-0.6 oder höher (SLES 9)
- *net-snmp* (Net-SNMP) Version 5.1.2-11.EL4.6 oder höher, inklusive *net-snmp-utils* (RHEL 4)

Eine genaue Beschreibung des Installationsvorgangs finden Sie im Handbuch *PRIMERGY ServerView Suite; Installation; ServerView V4.61*.



Beachten Sie bitte, dass die Services *atd* und entweder *inetd* oder *xinetd* aktiviert sein müssen. Diese Dienste können Sie über die Kommandozeilebene mit dem Kommando *chkconfig* aktivieren (siehe *man chkconfig*) oder über die jeweils installierte Systemverwaltungsapplikation:

1. SLES: *YaST2*
Rufen Sie *System* → *Runlevel Editor* auf.
2. RHEL: *Serviceconf*

Stellen Sie sicher, dass

- die Datei */etc/hosts* einen Eintrag mit der öffentliche IP-Adresse des Management-Servers und seinem Hostnamen enthält.
- Zeitzone und Systemzeit auf die lokale Zeit des Standortes eingestellt sind, an dem der Server betrieben wird (siehe *man hwclock*).

5.1.3 PRIMEQUEST-Partitionen mit Windows

Als Betriebssystem wird Windows Server 2003/2008 mit IA64 vorausgesetzt.

Folgende Software muss installiert sein:

- *PRIMEQUEST Sever Agent (PSA V1.9.0 oder höher)*, eine Software, die mit der PRIMEQUEST-Hardware geliefert wird



Die Auswirkungen einer DP-Aktion (Dynamische Partitionierung) sind in der Oberfläche des Performance Managers erst nach einem Neustart des Betriebssystems sichtbar.

5.1.4 PRIMEQUEST-Partition mit Linux

Als Betriebssystem wird mindestens SLES 9 SP2, RHEL 4 UR4 oder RHEL 5 (IA64-Version) vorausgesetzt.

Die folgenden Pakete müssen installiert sein:

- *at*
- *inetd* oder *xinetd*
- *openssl* (x86(i386)-Version)
- *compat-libstdc++-33* (V3.2.3-47.3 oder höher) (RHEL)
- *compat-libstdc++* (V5.0.7-22.2 oder höher) (SLES10)
- *ia32el*

- *FJSVpsa* (PSA V1.7.2 oder höher)
- *bash* (x86(i386)-Version)
- *net-snmp* (Net-SNMP) Version 5.1.3.1-0.6 oder höher (SLES 9)
- *net-snmp* (Net-SNMP) Version 5.1.2-11.EL4.6 oder höher, inklusive *net-snmp-utils* (RHEL 4)



Beachten Sie bitte, dass die Services *atd* und entweder *inetd* oder *xinetd* aktiviert sein müssen. Diese Dienste können Sie über die Kommandozeilebene mit dem Kommando *chkconfig* aktivieren (siehe *man chkconfig*) oder über die jeweils installierte Systemverwaltungsapplikation:

1. SLES: *YaST2*
Rufen Sie *System* → *Runlevel Editor* auf.
2. RHEL: *Serviceconf*

Stellen Sie sicher, dass

- die Datei */etc/hosts* einen Eintrag mit der öffentliche IP-Adresse des Management-Servers und seinem Hostnamen enthält.
- Zeitzone und Systemzeit auf die lokale Zeit des Standortes eingestellt sind, an dem der Server betrieben wird (siehe *man hwclock*).



Die Auswirkungen einer DP-Aktion (Dynamische Partitionierung) sind in der Oberfläche des Performance Managers erst nach einem Neustart des Betriebssystems sichtbar.

5.1.5 PRIMEPOWER mit Solaris

Als Betriebssystem wird Solaris 8 oder neuer vorausgesetzt.

Das folgende Paket muss installiert sein:

- *ESF 2.0* (*Enhanced Service Facility*) oder neuer

5.1.6 SPARC Enterprise Server mit Solaris

Als Betriebssystem wird Solaris 10 oder neuer vorausgesetzt.

Das folgende Paket muss installiert sein:

- *ESF 3.0 (Enhanced Service Facility)*

5.2 Installation

5.2.1 Installation auf PRIMEQUEST-Partitionen mit Windows

Vor der Installation der SNMP-ServerView-Agenten für Windows müssen Sie unbedingt die SNMP-Dienste im Betriebssystem installieren und aktivieren. Details werden im [Abschnitt „SNMP-Dienst installieren und aktivieren“ auf Seite 46](#) beschrieben.

Zur Installation der SVS EE-Agenten gehen Sie wie folgt vor:

- ▶ Wechseln Sie in das Verzeichnis *ServerView_Suite_Enterprise_Edition_Agent_Windows/all* und starten Sie das Programm *ServerViewAgents_Win_x64.exe*.
- ▶ Folgen Sie den Anleitungen auf dem Bildschirm.

Nach der Bestätigung der Lizenzvereinbarungen überprüft das Setup, ob schon eine ältere Version der SNMP-ServerView-Agenten auf dem Server installiert ist. In diesem Fall können Sie eine Upgrade-Installation vornehmen. Dabei wird die vorliegende Konfiguration gespeichert. Anschließend wird die alte Version gelöscht und die neue Version installiert. Hierbei wird die vorherige Konfiguration verwendet. Sie können in diesem Fall keine Änderungen vornehmen.

Falls noch keine Agenten-Installation vorliegt, wird das folgende Fenster geöffnet:

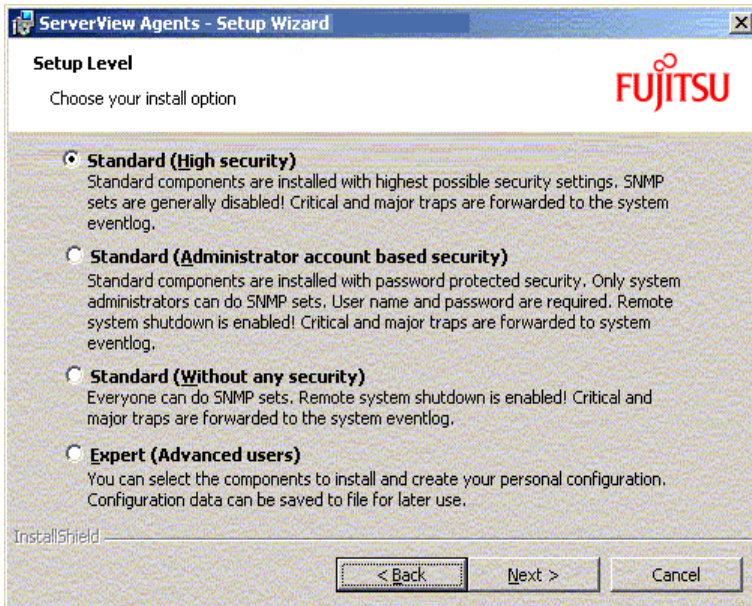


Bild 3: Fenster „Setup Level“

Das Setup bietet Ihnen vier vordefinierte Modi zur Agenteninstallation:

- Standard (High security)
- Standard (Administrator account based security)
- Standard (Without any security)
- Expert (Advanced users)

Wählen Sie den Modus *Standard (Without any security)*

Dieser Modus ist notwendig, wenn Sie die SVS EE Life Cycle-Komponenten (*Asset, Inventory, Performance, Update*) ohne Einschränkung nutzen wollen. Die Sicherheitseinstellungen werden durch eine SNMP-Dienste-Konfiguration im Betriebssystem bestimmt (siehe [Abschnitt „SNMP-Dienst installieren und aktivieren“ auf Seite 46](#)).

5.2.2 Installation auf PRIMERGY / PRIMEQUEST-Partitionen mit Linux

Das Produkt wird installiert, indem das Skript *installer* aus dem Verzeichnis *ServerView_Suite_Enterprise_Edition_Agent_Linux* aufgerufen wird.

Gehen Sie dazu wie folgt vor:

- ▶ Hängen Sie das ISO-Image in ein existierendes Verzeichnis ein, z. B. in */media*:

```
# mount -o loop <absolute_pathname_of_the_ISO_file> /media
```
- ▶ Wechseln Sie in das Verzeichnis des zu installierenden Produkts:

```
# cd /media/ServerView_Suite_Enterprise_Edition_Agent_Linux
```
- ▶ Starten Sie die Installation durch folgendes Kommando:

```
# ./installer
```

Ein Text wie der folgende erscheint:

```
+++ Installation of ServerView Suite Enterprise Edition started.
```

Folgen Sie den angezeigten Anweisungen.

- ▶ Wenn die Installation beendet ist, verlassen Sie das Einhänge-Verzeichnis und hängen Sie es aus, z. B.:

```
# cd /  
# umount /media
```

Eine Update-Installation berücksichtigt automatisch alle SVS EE Versionen ab V1.0.

5.2.3 Installation auf PRIMEPOWER / SPARC ES-Partitionen

Das Produkt wird installiert, indem das Skript *installer* aus dem Verzeichnis *ServerView_Suite_Enterprise_Edition_Agent_Solaris* aufgerufen wird.

Gehen Sie dazu wie folgt vor:

- ▶ Hängen Sie das ISO-Image in ein existierendes Verzeichnis ein, z. B. in */media*:

```
# device=`lofiadm -a <absolute_pathname_of_the_ISO_file>`  
# mount -F hsfs -o ro $device /media
```

- ▶ Wechseln Sie in das Verzeichnis des zu installierenden Produkts:

```
# cd /media/ServerView_Suite_Enterprise_Edition_Agent_Solaris
```

- ▶ Starten Sie die Installation durch folgendes Kommando:

```
# ./installer
```

Ein Text wie der folgende erscheint:

```
+++ Installation of ServerView Suite Enterprise Edition started.
```

Folgen Sie den angezeigten Anweisungen.

- ▶ Wenn die Installation beendet ist, verlassen Sie das Einhänge-Verzeichnis und hängen Sie es aus, z. B.:

```
# cd /  
# umount /media  
# lofiadm -d $device
```

Eine Update-Installation berücksichtigt automatisch alle PW SVS Versionen ab V2.2B10.

5.2.3.1 “LiveUpgrade”-Installation des Solaris ServerView Agenten

Gehen Sie wie folgt vor, wenn Sie die *LiveUpgrade*-Fähigkeit der Solaris ServerView-Agenten einsetzen möchten:

- ▶ Hängen Sie die Platte mit dem aktualisierten Betriebssystem in einen bereits vorhandenen Root-Pfad ein.
- ▶ Starten Sie die Installation des Solaris-ServerView-Agenten auf die Platte mit dem aktualisierten Betriebssystem mit folgendem Kommando:
./installer -R <pathname>
wobei <pathname> der Root-Pfad zum Betriebssystem auf der neu eingehängten Platte ist.

Alternativ zur Option *-R <pathname>* können Sie diesen Pfad mit Hilfe der Umgebungsvariablen *\$PKG_INSTALL_ROOT* spezifizieren.

Wenn das neue Betriebssystem mit dem Solaris-ServerView-Agenten aktualisiert wurde, können Sie mit einem Neustart von der Platte mit dem auf diese Weise vorbereiteten Betriebssystem auf das neue System umschalten.

5.3 Deinstallation

Wenn Sie die Agenten-Software auf einem überwachten System deinstallieren wollen, sollten Sie das betreffende System über das GUI zuerst aus der Verwaltungsdomäne entfernen.

5.3.1 Deinstallation auf Windows-Systemen

Entfernen Sie die *ServerView Agents* mit Hilfe der Systemverwaltungsfunktion *Start → Systemsteuerung → Software → Programme hinzufügen/entfernen*.

5.3.2 Deinstallation auf Linux-Systemen

Das Agenten-Produkt wird deinstalliert, indem das Skript *deinstaller.ServerView_Suite_Enterprise_Edition_Agent_Linux* im Verzeichnis */opt/SMAW* aufgerufen wird.

5.3.3 Deinstallation auf Solaris-Systemen

Das Produkt wird deinstalliert, indem das Skript *deinstaller.ServerView_Suite_Enterprise_Edition_Agent_Solaris* aus dem Verzeichnis */opt/SMAW* aufgerufen wird.

5.4 Konfiguration

Der SNMP-Dienst auf den verwalteten Systemen muss so eingerichtet sein, dass er die von der *ServerViewSuite* gesendeten SNMP-Aufträge zulässt. Nähere Informationen zur SNMP-Konfiguration finden Sie im [Kapitel „SNMP-Konfiguration“ auf Seite 39](#).

Die *ServerViewSuite* kommuniziert mit den verwalteten Knoten über TCP/IP und über SNMP. Hierzu werden Ports auf dem Management-Server und den verwalteten Knoten belegt.

Werden die Standardbelegung der fest zugewiesenen Ports oder die Bereiche für die dynamisch zugewiesenen Ports geändert, so müssen auch auf den verwalteten Knoten Anpassungen vorgenommen werden. Nähere Informationen hierzu finden Sie im [Kapitel „Portkonfiguration“ auf Seite 59](#).

Sollen durch die *ServerViewSuite* PRIMEQUEST-Systeme verwaltet werden, so müssen über den MMB der PRIMEQUEST einige Anpassungen vorgenommen werden. Die Konfigurationsschritte sind im [Abschnitt „Einstellungen im MMB-Web UI“ auf Seite 69](#) beschrieben.

Um ein SPARC-Enterprise-System durch SVS EE zu verwalten, müssen über das XSCF-Board Anpassungen vorgenommen werden. Nähere Informationen finden Sie im [Kapitel „SPARC ES konfigurieren“ auf Seite 83](#).

Soll ein Unix-Knoten in eine sichere Domäne aufgenommen werden, so muss der öffentliche Schlüssel des SVS EE-Benutzers im Verzeichnis `/opt/SMAW/.cert/<user>` installiert werden. Nähere Informationen finden Sie im [Kapitel „Kommunikationswege absichern“ auf Seite 49](#).

6 SNMP-Konfiguration

Da die Überwachungsfunktionen der *ServerView Suite* auf die SNMP-Schnittstelle zugreifen, müssen die SNMP-Agenten entsprechend auf jedem verwalteten Knoten installiert und konfiguriert werden.

Auf dem Management-Server werden SNMP-Aufträge an die verwalteten Knoten gesendet und Traps von den verwalteten Knoten empfangen.

Bei der Installation und Konfiguration der SNMP-Dienste werden Ihnen Standardwerte angeboten. Sie erhöhen die Sicherheit auf dem verwalteten Knoten, indem Sie die Standardwerte des SNMP-Dienstes modifizieren. Die Änderungen müssen jedoch immer sowohl auf den verwalteten Knoten als auch auf dem Management-Server erfolgen.

Folgende Parameter können konfiguriert werden:

- Community-Name für eingehende SNMP-Anfragen

Der Community-Name (Community string) ist Bestandteil eines jeden SNMP-Requests, der vom Manager an den Agenten geschickt wird.

Standardmäßig wird der Community-Name *public* vergeben. Dieser Standardwert wird von den meisten SNMP-Diensten genutzt. Es ist aus Sicherheitsgründen sinnvoll, den Wert zu ändern. Sie können für jeden Server bzw. für Servergruppen eine individuelle Community definieren.

- Rechte für die Community

Der Community können Rechte zugeordnet werden (z.B. *read-only*, *read-write*). Wenn Sie die gesamte ServerView Funktionalität nutzen wollen, so müssen Sie der Community die Rechte *read-write* geben. Sie schränken die Funktionalität, wenn Sie nur lesenden Zugriff zulassen (*read-only*).

Der ServerView-Manager unterstützt pro verwalteten Knoten nur eine Community für SNMP-Requests. Deshalb können Sie keine verschiedenen Communities mit unterschiedlichen Rechten für einen verwalteten Knoten konfigurieren. Außerdem muss für alle Partitionen eines PRIMEQUEST-Systems die Community des MMB verwendet werden. Auch für alle Blades eines Blade-Servers muss dieselbe Community des Management-Blades verwendet werden.

- SNMP-Anfragen von ausgewählten/allen Servern erlauben

Es ist sinnvoll, nur die IP-Adresse des Servers einzutragen, der als Management-Server fungieren soll. Damit wird verhindert, dass der Agent Anfragen von nicht berechtigten Servern akzeptiert.

- Trap-Zielsystem

IP-Adresse des Management-Servers, an den die SNMP-ServerView-Agenten Traps senden.



Wenn Sie auf einem verwalteten Knoten für den SVS EE-Management-Server keine SNMP-Schreibrechte vergeben, so sind folgende Funktionen des Performance-Managements nicht nutzbar:

- Setzen von Schwellwerten
- Definieren von Reports

Eine Auswertung von bereits existierenden Schwellwert- und Report-Settings des verwalteten Knoten (die definiert wurden, als Schreibrechte existierten) ist auch ohne Schreibrechte möglich.

6.1 SNMP-Konfiguration auf dem Management-Server

Auf dem Management-Server werden SNMP-Aufträge (Lese- und Schreibaufträge) an die verwalteten Knoten gesendet und Traps von den verwalteten Knoten empfangen.

Die SNMP-Aufträge werden an Port 161 gesendet, die Traps auf Port 162 empfangen. Eine Änderung dieser Ports ist nicht zulässig.

Die Community, mit der die SNMP-Aufträge gesendet werden, wird für jeden verwalteten Knoten bei der Aufnahme dieses Knotens in die SVS EE-Verwaltungsdomäne festgelegt (Eingabefeld *Community name* in der Dialogbox zum Anlegen eines PRIMERGY-, PRIMEQUEST- oder Linux-Servers). Für alle Partitionen eines PRIMEQUEST-Systems muss die Community des MMB verwendet werden. Auch für alle Blades eines Blade-Servers muss dieselbe Community des Management-Blades verwendet werden.

Soll die Community später geändert werden, so muss der entsprechende Knoten aus der Domäne entfernt und mit Angabe der neuen Community wieder angelegt werden.

Die Standardkonfiguration arbeitet mit der Community *public*. Wenn Sie eine andere Community angeben, so müssen Sie dies auf dem verwalteten System ebenfalls konfigurieren.

6.2 SNMP-Konfiguration auf den verwalteten Knoten

Die SNMP-ServerView-Agenten sind auf Basis des SNMP-Master-Agenten (systemspezifischer SNMP-Agent) geschrieben, d. h. das Empfangen von SNMP-Aufträgen und das Senden der Traps erfolgt unter Kontrolle des SNMP-Master-Agenten. Deshalb ist es wichtig, den SNMP-Master-Agenten so zu konfigurieren, dass

- die Traps an den Management-Server gesendet werden und
- die SNMP-Aufträge (lesen und schreiben) des Management-Servers akzeptiert werden

Die SNMP-Aufträge werden an Port 161 empfangen, die Traps an Port 162 gesendet. Eine Änderung dieser Ports ist nicht zulässig.

6.2.1 Linux-System

Auf Linux-Systemen müssen

- der SNMP-Master-Agent konfiguriert werden
- die SNMP-ServerView-Agenten konfiguriert werden

Anschließend stoppen und starten Sie die Agenten, damit die Änderungen wirksam werden:

```
# /etc/init.d/srvmagt stop
# /etc/init.d/snmpd stop
# /etc/init.d/snmpd start
# /etc/init.d/srvmagt start
```

Außerdem müssen Sie sicher stellen, dass nach einem Neustart des Systems die SNMP-Master-Agenten und die SNMP-ServerView-Agenten automatisch gestartet werden.

6.2.1.1 Konfiguration des SNMP-Master-Agenten

Der SNMP-Master-Agent sucht die Konfigurationsdatei im Verzeichnis:

Linux	SNMP-Konfigurationsdatei
SUSE, SLES 9	/etc/snmpd.conf
SUSE, SLES 10	/etc/snmp/snmpd.conf
Red Hat, RHEL	/etc/snmp/snmpd.conf

Tabelle 1: Speicherorte, an denen der SNMP-Master-Agent seine Konfigurationsdatei erwartet

Erweitern Sie *snmpd.conf* so, dass der SVS EE-Manager als Trap-Ziel festgelegt wird und Lese-/Schreibberechtigung erhält. Sie können die Konfigurationsdatei mit einem Texteditor wie *vi* bearbeiten. Näheres über die Syntax finden Sie in der Manual Page *snmpd.conf*(5).

i

Änderungen in der Konfigurationsdatei treten erst nach einem Neustart des SNMP-Master-Agenten in Kraft.

Es wird empfohlen, folgende Werte in *snmpd.conf* zu setzen:

Variable	Erläuterung
<i>syscontact</i>	Kontaktdaten des zuständigen Administrators (Name, Mail-adresse, Telefonnummer).
<i>syslocation</i>	Standort des verwalteten Knotens.
<i>authtrapenable</i>	Trap bei fehlgeschlagenen Authentifizierungen senden: 1 (enable, empfohlener Wert) 2 (disable, Standardwert)

Tabelle 2: Werte, die in der Datei *snmpd.conf* spezifiziert werden sollten

Ergänzen Sie die *snmpd.conf* gemäß dem folgenden Template. Es beschreibt eine Konfiguration, die SNMP-get- und set-Befehle zulässt und Traps an den *<host>* sendet. Tragen Sie für *<host>* die IP-Adresse des SVS EE-Managers ein.

```
com2sec svSec 127.0.0.1 public
com2sec svSec localhost public
com2sec svSec <host> public
group svGroup v1 svSec
view svView included .1
access svGroup "" any noauth exact svView svView none
trapsink <host> public
```



Wenn Sie nur Lese-Rechte zulassen wollen, muss die vorletzte Zeile wie folgt geändert werden:

```
access svGroup "" any noauth exact svView none none
```



Der Name der Community in unserem Beispiel lautet *public*. Wenn Sie aus Sicherheitsgründen einen anderen Community-Namen benutzen wollen, ersetzen Sie *public* durch den Namen Ihrer Wahl. Konfigurieren Sie den Community-Namen in dem Fall auch managerseitig (siehe [Abschnitt „SNMP-Konfiguration auf dem Management-Server“ auf Seite 40](#)). Für alle Partitionen eines PRIMEQUEST-Servers (bzw. alle Blades eines Blade-Servers) muss jeweils dieselbe Community verwendet werden.



Die Reihenfolge der *com2sec*-Definitionen ist wichtig. Sie geht von spezifischen IP-Adressen zu generischen IP-Adressen innerhalb derselben Community. Soll der Zugriff nicht nur speziellen Knoten sondern einem ganzen Subnetz gestattet werden, so müssen die *com2sec*-Zeilen mit der Subnetz-Angabe (<subnet>/<netmask>) nach den *host*-Zeilen folgen. Bitte beachten Sie:

1. Stellen Sie sicher, dass die Zeilen

```
com2sec svSec 127.0.0.1 public
com2sec svSec localhost public
```

vor der Zeile

```
com2sec psalocal localhost psaprivate
```

stehen.

2. Falls die Datei *snmpd.conf* die Zeile

```
com2sec notConfigUser default public
```

enthält, so löschen Sie sie oder verlagern sie hinter die oben beschriebenen *com2sec*-Zeilen für *svSec*.

Mit *trapsink* legen Sie die Zieladressen für SNMP-Traps fest. Geben Sie für jedes Trap-Ziel eine Zeile mit der IP-Adresse oder dem Hostnamen des Ziels ein.

6.2.1.2 Konfiguration der SNMP-ServerView-Agenten

Die Konfigurationsdatei für die SNMP-ServerView-Agenten ist */etc/srvmagt/config*.



Änderungen in der Konfigurationsdatei treten erst nach einem Neustart der SNMP-ServerView-Agenten in Kraft.

In der mitgelieferten Version von */etc/srvmagt/config* sollten Sie folgende Werte setzen, um den vollen Funktionsumfang des Performance-Managements nutzen zu können:

`NoAccountCheck =1`

`AgentPermission=3`

Dadurch erlauben Sie SNMP-Set-Operationen ohne Passwort-Abfrage auf dem verwalteten Server. Diese Angaben sind zusätzlich zu der *access*-Angabe in *snmpd.conf* (siehe [Abschnitt „Konfiguration des SNMP-Master-Agenten“ auf Seite 42](#)) erforderlich.

Eine detaillierte Erläuterung der Datei */etc/srvmagt/config* befindet sich im [Abschnitt „Konfiguration der SV-SNMP-Agenten unter Linux“ auf Seite 91](#).

6.2.1.3 Starten und Stoppen der SNMP-Agenten

Damit die Änderungen an den Konfigurationsdateien wirksam werden, müssen die Agenten neu gestartet werden. Sie können dies durch Kommandoeingabe oder durch einen Neustart des Systems erreichen. Zuvor muss der automatische Start der Agenten für den Systemstart eingerichtet werden.

Automatischer Start

Der automatische Start für den SNMP-Master-Agenten *snmpd* und den SNMP-ServerView-Agenten *srvmagt* muss aktiviert werden. Dies können Sie mit Hilfe des jeweiligen Systemverwaltungsprogramms oder durch folgende Kommandos durchführen.

```
# chkconfig snmpd on
```

```
# chkconfig srvmagt on
```

Alternativ über Systemverwaltungsprogramm:

Für SUSE-Systeme:

- ▶ Führen Sie YaST aus und wählen Sie *System* → *Runlevel Editor*
- ▶ Setzen Sie *snmpd* und *srvmagt* auf *enable* und speichern Sie diese Einstellung

- ▶ Setzen Sie den Betriebssystemmodus auf mindestens 3

Für Red Hat-Systeme:

- ▶ Starten Sie das *Service Configuration Tool* über Anwahl von *Systemeinstellungen* → *Servereinstellungen* → *Dienste*
- ▶ Setzen Sie *snmpd* und *srvmagt* auf *enable*, indem Sie die Box neben dem Namen anklicken, und speichern Sie diese Einstellung
- ▶ Setzen Sie den Betriebssystemmodus auf mindestens 3

Manueller Start

Der SNMP-Master-Agent *snmpd* muss gestartet sein, damit SNMP-ServerView-Agenten gestartet werden können. Die SNMP-ServerView-Agenten sollten gestoppt werden, bevor der *snmpd* gestoppt wird:

```
# /etc/init.d/srvmagt stop
# /etc/init.d/snmpd stop
# /etc/init.d/snmpd start
# /etc/init.d/srvmagt start
```

6.2.2 Windows-System

Hier wird nur die Installation für die PRIMEQUEST-Partition (mit Windows 2003/2008) beschrieben. Die Installation der SNMP-ServerView-Agenten auf PRIMERGY-Systeme entnehmen Sie bitte dem Handbuch *PRIMERGY ServerView Suite – Installation unter Windows – ServerView V4.60*.

Vor der Installation der SNMP-ServerView-Agenten für Windows müssen Sie unbedingt die SNMP-Dienste im Betriebssystem installieren und aktivieren. Andernfalls kann der Management-Server die verwalteten Knoten nicht überwachen.

6.2.2.1 SNMP-Dienst installieren und aktivieren

Zur Aktivierung des SNMP-Dienstes, müssen Sie folgende Schritte vornehmen, sofern Sie dies nicht bereits während der Systeminstallation durchgeführt haben:

1. Installation

- ▶ Rufen Sie zur Installation *Start → Einstellungen → Systemsteuerung → Windows-Komponenten hinzufügen/entfernen* auf (Pfad ist OS-abhängig!).
- ▶ Markieren Sie im Fenster *Windows-Komponenten* den Eintrag *Verwaltungs- und Überwachungsprogramme* und klicken dann auf die Schaltfläche *Details*.
- ▶ Markieren Sie den Eintrag *SNMP (Simple Network Management Protocol)* und klicken dann auf die Schaltfläche *OK* und *Weiter*.

2. Konfiguration

- ▶ Rufen Sie zur Konfiguration *Start → Einstellungen → Systemsteuerung → Verwaltung → Komponentendienste* auf.
- ▶ Markieren Sie den Dienst *SNMP-Dienst* und wählen Sie aus dem Kontextmenü den Eintrag *Eigenschaften*.
 - ▶ Tragen Sie in der Registerkarte *Traps* unter *Communityname* einen Namen ein.

Mit *Communityname* wird die Zugriffsberechtigung des Management-Servers gesteuert. Nur Abfragen mit dieser Community werden zugelassen. Dieser Wert muss mit der Community-Angabe übereinstimmen, die im GUI beim Anlegen des verwalteten Knotens in der SVS EE-Domäne gemacht wird.

- ▶ Tragen Sie unter *Trapziele* mit *Hinzufügen* die IP-Adresse des Management-Servers für die angegebene Community ein. Traps werden nur an die hier eingetragenen Management-Server gesendet.
- ▶ Registerkarte *Sicherheit*:
 - ▶ Setzen Sie die *Rechte* für die Community auf *LESEN SCHREIBEN*.
 - ▶ *SNMP-Pakete von jedem Host annehmen/ SNMP-Pakete von diesen Hosts annehmen*:

Hier können Sie Server auswählen, von denen SNMP-Pakete akzeptiert werden sollen, oder alle auswählen. Tragen Sie hier den Management-Server ein.



Da SNMP ein offenes Protokoll ohne Passwortsicherung ist, sollten nur die Management-Server eingetragen werden, die auch als solche fungieren sollen. Unbefugte Teilnehmer des Netzes könnten sonst wichtige Parameter des Systems verändern und damit den Server-Betrieb stören.

- Klicken Sie auf *OK*.

3. Starten

- Starten Sie den SNMP-Dienst unter *Dienste*. Wählen Sie dazu *Starten* aus dem Kontextmenü.

6.2.2.2 SNMP-ServerView-Agenten aktivieren

Um nachträglich die bei der Installation vorgenommene Standardkonfiguration der SNMP-ServerView-Agenten zu ändern, starten Sie unter *Start* → *All Programs* → *Fujitsu* → *ServerView* → *Agents* → *Configuration* → *Agent Configuration* und folgen den Anleitungen auf dem Bildschirm. Nähere Informationen sind im [Abschnitt „Konfiguration der SV-SNMP-Agenten unter Windows“ auf Seite 93](#) aufgeführt.

7 Kommunikationswege absichern

Die *ServerView Suite* nutzt zwei Wege zur Absicherung der Kommunikation:

- SSL, um die TCP/IP-Verbindungen abzusichern
- HTTPS, um die Web-Verbindungen abzusichern

Beide Wege können unabhängig voneinander konfiguriert werden.

Für eine Absicherung aller Kommunikationsvorgänge müssen beide Konfigurationen vorgenommen werden.

7.1 SSL für TCP/IP-Verbindungen

Die *ServerView Suite* kann das SSL-Protokoll für eine sichere Erweiterung des Standard-TCP/IP-Protokolls verwenden. Die sichere Socket-Schicht wird zwischen der Transportschicht und der Anwendungsschicht des Standard-TCP/IP-Protokoll-Stacks eingefügt. Die SSL-basierte Kommunikation zwischen allen Komponenten verwendet eine Authentifizierung mit öffentlichen/privaten Schlüsseln auf der Grundlage von X509-Zertifikaten.

Die Kommunikation über SSL beginnt mit einem Informationsaustausch zwischen dem Verwaltungsarbeitsplatz und dem Management-Server. Dieser Austausch von Informationen wird als SSL-Handshake bezeichnet. Im weiteren Verlauf wird auch die Kommunikation zwischen dem Management-Server und den verwalteten UNIX-Knoten (Linux und Solaris) über SSL abgesichert.

Im folgenden werden alle Schritte erläutert, die zum Aufbau einer sicheren Domäne notwendig sind.

7.1.1 Aufbau einer sicheren Domäne

Für den Aufbau einer sicheren Administrationsdomäne muss der Systemadministrator folgende Schritte ausführen:

1. Berücksichtigen Sie die Anzahl Verwaltungsarbeitsplätze und verwalteten Knoten in Ihrer Domäne.
2. Berücksichtigen Sie die Anzahl Benutzer, die eine Zugriffsberechtigung bekommen sollen.
3. Erstellen Sie die erforderlichen Zertifikate und Schlüssel für jeden Benutzer auf dem Management-Server. Jeder Benutzer sollte sein eigenes Zertifikat, PEM-Zertifikat und Schlüssel bekommen. Nähere Informationen finden Sie im [Abschnitt „Aufbau eines selbstsignierten Benutzerzertifikats“ auf Seite 51](#).
4. Verteilen Sie die Zertifikate *WSA_cert.pem* und die Hash-Datei „*.0“ auf einem sicheren Weg an alle verwalteten Knoten und dem Management-Server (Verzeichnis */opt/SMAW/.cert/<user>*).
5. Kopieren Sie die privaten Schlüssel *WSA_key.pem*, Zertifikate und Hash-Dateien auf einem sicheren Weg auf den Management-Server (Verzeichnis *\$HOME/.cert_private*).
6. Verteilen Sie das Client-Zertifikat *wsa_cert.p12* auf einem sicheren Weg an alle Verwaltungsarbeitsplätze, die eine Zugriffsberechtigung für diese Domäne bekommen sollen (Verzeichnis */opt/SMAW/wsa_certs/<user>* oder *C:\wsa_certs\<user>*, siehe auch den Absatz „[Verwaltungsarbeitsplatz](#)“ auf [Seite 54](#)).
7. Starten Sie *ServerView Suite* und erzeugen Sie die Administrationsdomäne.

Es sind folgende Einschränkungen zu berücksichtigen:

- Die Verteilung der Schlüssel und Zertifikate muss manuell erfolgen und erfordert Root-Berechtigung auf allen Systemen. Anschließend sollte die Domäne mit der *ServerView Suite* erstellt werden.
- Eine Mischung von sicheren und nicht sicheren Rechnern wird nicht unterstützt.
- Nicht sichere Verwaltungsarbeitsplätze werden keinen Zugriff mehr auf eine Domäne haben, die sicher geworden ist.

7.1.2 Aufbau eines selbstsignierten Benutzerzertifikats

Das Benutzerzertifikat kann durch Aufruf des interaktiven Kommandos *MK-KEY* oder durch Verwendung von *openssl*-Kommandos erzeugt werden. Beide Verfahren sind im folgenden beschrieben.

Am Ende müssen folgende Dateien erzeugt sein:

```
$HOME/.cert_private/WSA_key.pem  
$HOME/.cert_private/WSA_cert.pem  
  
/opt/MAW/.cert/$USER/WSA_cert.pem  
/opt/MAW/.cert/$USER/[hash.0] -> WSA_cert.pem  
  
/opt/MAW/.cert/$USER/wsa_cert.p12
```

7.1.2.1 Verwendung von MK_KEY

Loggen Sie sich auf dem Management-Server mit der User-Berechtigung ein, über die Sie die SVS EE ausführen wollen.

Rufen Sie folgendes Kommando auf:

```
# /opt/MAW/MAWssl/bin/MK_KEY -i
```

Folgen Sie den Anweisungen auf dem Bildschirm.

Bei den folgenden Aufforderungen

```
Enter pass phrase for WSA_key.pem:  
Enter Export Password:
```

geben Sie jeweils dasselbe Passwort ein. Dieses Passwort müssen Sie dann als PEM-Passwort in der Login-Maske von SVS EE eingeben (siehe [Abschnitt „Anmeldeverfahren“ auf Seite 55](#)).

7.1.2.2 Verwendung der openssl-Kommandos

Das Programm *openssl* hat eine Kommandoschnittstelle für die verschiedenen Verschlüsselungsfunktionen der OpenSSL-Verschlüsselungsbibliothek auf Shell-Ebene. Es kann folgendermaßen verwendet werden:

- Erzeugung von RSA-, DH- und DSA-Schlüsselparametern
- Erzeugung von X.509-Zertifikaten, CSRs und CRLs

Loggen Sie sich auf dem Management-Server mit der User-Berechtigung ein, über die Sie die SVS EE ausführen wollen.

1. Erzeugung des privaten Schlüssels:

Wenn */dev/urandom* verfügbar ist, dann muss der private Schlüssel mit folgendem Befehl hergestellt werden:

```
# /opt/SMAW/SMAWssl/bin/openssl genrsa -des3 -out \  
$HOME/.cert_private/WSA_key.pem 2048
```

Wenn */dev/urandom* nicht verfügbar ist, dann muss der private Schlüssel mit folgendem Befehl erzeugt werden:

```
# /opt/SMAW/SMAWssl/bin/openssl genrsa -des3 -out \  
$HOME/.cert_private/WSA_key.pem -rand \  
/opt/SMAW/SMAWwsaS/conf/prngsock 2048
```

/opt/SMAW/SMAWwsaS/conf/prngsock ist ein alternativer Zufallsgenerator, der installiert ist, falls */dev/urandom* nicht verfügbar ist.

2. Erzeugung des selbstsignierten Wurzelzertifikats:

Geben Sie folgendes Kommando ein:

```
# /opt/SMAW/SMAWssl/bin/openssl req -new -x509 -days 730 \  
-key $HOME/.cert_private/WSA_key.pem -out \  
$HOME/.cert_private/WSA_cert.pem
```

Die Option *-days* beschreibt die Anzahl Tage bis zum Verfallsdatum des Zertifikats. Das Wurzelzertifikat muss auch nach */opt/SMAW/.cert/<user>* kopiert werden.

```
# cp $HOME/.cert_private/WSA_cert.pem /opt/SMAW/.cert/<user>
```

3. Indizierung des Zertifikat-Subjektnamens:

Die Subjektnamen der Zertifikate werden in OpenSSL für einen Index verwendet, in dem alle Zertifikate nach ihren Subjektnamen gesucht werden können.

Führen Sie folgende Kommandos aus:

```
# cd /opt/SMAW/.cert/<user>
```

```
# ln -s WSA_cert.pem `openssl x509 -hash -noout -in \  
WSA_cert.pem`.0
```

4. Erzeugung einer PKCS12-Datei für das GUI:

Das Kommando *pkcs12* ermöglicht es, PKCS#12-Dateien (die manchmal auch als PFX-Dateien bezeichnet werden) zu erstellen und zu analysieren. PKCS#12-Dateien werden von mehreren Programmen wie zum Beispiel Netscape, MS Internet Explorer und MS Outlook verwendet.

Führen Sie folgende Kommandos aus:

```
# cd /opt/SMAW/.cert/<user>

# /opt/SMAW/SMAWssl/bin/openssl pkcs12 -export -in \
WSA_cert.pem -inkey /root/.cert_private/WSA_key.pem \
-out wsa_cert.p12
```

7.1.3 Installation von öffentlichen und privaten Schlüsseln

Für jeden Benutzer, der sich bei der *ServerView Suite* anmelden möchte, wird ein Paar von öffentlichen und privaten Schlüsseln installiert. Die öffentlichen und privaten Schlüssel müssen auf den verschiedenen Arten von Systemen, die an der Kommunikation innerhalb der *ServerView Suite* beteiligt sind, folgendermaßen installiert sein:

1. Management-Server

Der Management-Server benötigt beide Schlüssel: den öffentlichen und den privaten Schlüssel:

Kopieren Sie die öffentlichen Schlüssel-Dateien *WSA_cert.pem*, *<hash>.0* und *wsa_cert.p12* in das Verzeichnis */opt/SMAW/.cert/<user>*.

Kopieren Sie die privaten Schlüssel-Dateien *WSA_key.pem* und *WSA_cert.pem* in das Verzeichnis *\$HOME/.cert_private*.

Schränken Sie die Zugriffsrechte für *\$HOME/.cert_private* auf Leserechte für *root* und den Benutzer selbst ein.

2. Verwaltete Knoten

Bei diesen Knoten muss nur der öffentliche Schlüssel des Login-Users installiert sein.

Kopieren Sie die Dateien *WSA_cert.pem* und *<hash>.0* in das Verzeichnis */opt/SMAW/.cert/<user>*.

Stellen Sie sicher, dass das Verzeichnis */opt/SMAW/.cert* nur privilegierten Benutzern (z. B. *root*) zugänglich ist.



Auf diesem Weg bekommt der Login-User, d. h. der Eigentümer des öffentlichen Schlüssels, Root-Berechtigung auf diesem Knoten. Daher muss gewährleistet sein, dass das Installationsverzeichnis */opt/SMAW/.cert* des öffentlichen Schlüssels nur sehr beschränkte

Zugriffsrechte hat. Die Root-Rechte werden von *ServerView Suite* benötigt, um Systemadministrations- und Konfigurationsaufgaben zu erledigen.

3. Verwaltungsarbeitsplatz

Auf dem Verwaltungsarbeitsplatz muss nur der private Schlüssel des Benutzers installiert werden.

Kopieren Sie die Datei *wsa_cert.p12* in das systemspezifische Installationsverzeichnis:

Windows: *C:\wsa_certs\<user>*

Unix: */opt/SMAW/wsa_certs/<user>*

Falls ein Benutzer mehrere Domänen verwaltet und deshalb mehrere Zertifikate benötigt, so erzeugen Sie im Installationsverzeichnis ein Unterverzeichnis mit dem Namen des Management-Servers (*C:\wsa_certs\<user>\<servername>*) und kopieren die Schlüsseldatei in dieses Unterverzeichnis.



Wenn das benötigte Zertifikat

wsa_certs/<user>/<servername>/wsa_cert.p12 nicht existiert, wird auf das Zertifikat in dem übergeordneten Verzeichnis *wsa_certs/<user>/wsa_cert.p12* zurückgegriffen.

7.1.4 Anmeldeverfahren

Ein Benutzer der SVS EE muss sich mit einer gültigen Benutzerkennung des Management-Servers und dem zugehörigen Passwort anmelden. Für sichere Verbindungen muss der Benutzer zusätzlich das PEM-Passwort der privaten Schlüsseldatei eingeben:

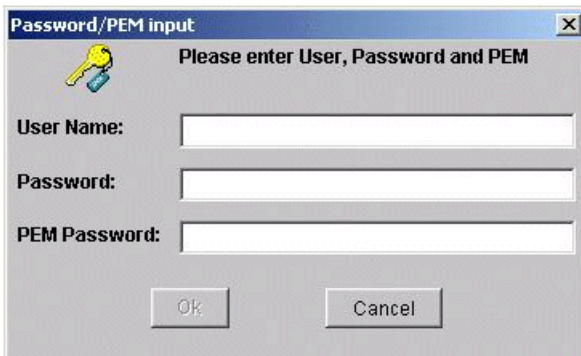


Bild 4: Dialogbox für Login mit SSL

Das GUI benutzt dieses Passwort, um die private Schlüsseldatei des betroffenen Benutzers auf dem Verwaltungsarbeitsplatzes zu lesen. Diese private Schlüsseldatei wird verwendet, um den Benutzer beim Management-Server mit Hilfe des sogenannten SSL-Handshake-Protokolls zu authentifizieren. Nachdem die Verbindung aufgebaut wurde, sendet das GUI das private Schlüsselpasswort an den Management-Server, so dass die private Schlüsseldatei auf dem Verwaltungsarbeitsplatz geöffnet werden kann.



Da die Kommunikation zwischen Management-Station und Verwaltungsarbeitsplätze SSL verwendet, wird das private Schlüsselpasswort über eine sichere Verbindung gesendet. Dies funktioniert nur, wenn die privaten Schlüsseldateien auf dem Management-Server und auf dem Verwaltungsarbeitsplatz übereinstimmen.

Nach dem Anmeldeverfahren ist die Kommunikation zwischen Verwaltungsarbeitsplatz und Management-Server sicher und der Management-Server hat alle Informationen, um gegebenenfalls eine SSL-basierte Kommunikation mit den verwalteten Knoten aufzubauen. Man erkennt dies am Icon unten links, das jetzt ein geschlossenes Schloss zeigt:



Bild 5: Icon für SSL-Verbindung

Besteht keine sichere Verbindung, ist das Schloss geöffnet.

7.1.5 Fehlersituationen

In diesem Abschnitt werden einige Fälle beschrieben, in denen eine sichere Kommunikation nicht möglich ist. Das bedeutet, dass keine Kommunikation zwischen den beteiligten Komponenten der *ServerView Suite* aufgebaut wird.

1. Der verwaltete Knoten enthält nicht den öffentlichen Schlüssel in dem speziellen Benutzerverzeichnis

Wenn dieser Knoten bereits Teil einer Domäne ist (zum Beispiel aufgrund der Verwendung älterer Versionen), dann wird dieser Knoten grau (inaktiv) im GUI dargestellt. Eine Kommunikation mit diesem Knoten wird nicht aufgebaut.

2. Der Management-Server hat keine privaten Schlüssel

Dies bedeutet, dass der Management-Server nicht in der Lage ist, sich bei dem verwalteten Knoten zu authentifizieren. Ein solcher Management-Server ist nicht einsetzbar. Ein Login bei diesem Management-Server unter Verwendung der *ServerView Suite* über eine SSL-Verbindung ist nicht möglich.

3. Der Management-Server hat keine öffentlichen Schlüssel für den Login-User

Der Benutzer ist nicht in der Lage, sich beim Management-Server anzumelden. Dieser Benutzer darf diesen Server nicht zum Verwalten der Domäne verwenden.

7.2 Kommunikation mittels HTTPS absichern

Um beim Aufruf der Life Cycle Modules die Kommunikation des Verwaltungsarbeitsplatzes mit den Management-Server abzusichern, muss das HTTPS-Protokoll aktiviert werden. Hierfür sind die folgenden Maßnahmen erforderlich:

- ▶ Aktivieren Sie im Apache Webserver das SSL-Modul auf dem Management-Server (nähere Informationen entnehmen Sie bitte dem Systemmanual für Linux-Administration).
- ▶ Wählen Sie in der Oberfläche der SVS EE unter dem Menüpunkt *Edit* in der Menüleiste die Aktion *Preferences* aus und wechseln Sie in die Registerkarte *WebAccess*. In der anschließenden Dialogbox aktivieren Sie die Einstellung *Use SSL*. Der Port verändert sich automatisch auf 443.



Bild 6: SSL-Einstellung setzen

8 Portkonfiguration

8.1 Fest zugewiesene Ports

In den Dateien */etc/services* und *http_addWSA.conf* werden Ports fest zugewiesen. Bereiche für dynamisch zugewiesene Ports werden in produktspezifischen Dateien festgelegt. Die Standardinstallation verwendet die folgenden Portlisten:

- 80 (TCP) (Life Cycle Management)
- 161 (UDP/TCP) (SNMP-Dienst)
- 162 (UDP/TCP) (SNMP-Trapempfang)
- 8886 (UDP) (WSA Server)
- 8899 (UDP) (Domain Admin)
- 8881-8883 (TCP) (WebService)
- 3172 (Performance Management)
- 23460 (SSH-Kommunikation)

8.1.1 Fest zugewiesene Ports auf dem Management-Server

Bei der Installation der *ServerView Suite* werden in der Datei */etc/services* folgende Einträge erstellt:

WSAserver	8886/udp	#Serververwaltung
dom_adm	8899/udp	#Port für Domänenverwaltungsservice

Tabelle 3: Beim Start der *ServerView Suite* in der Datei */etc/services* angelegte Einträge

Die Zuordnung des Ports 162 darf nicht geändert werden. Falls *snmptrapd* läuft, wird der Prozess angehalten und auf Port 8162 neu gestartet.

Die oben genannten Ports sind für *ServerView Suite* unerlässlich.

Für Webserver-Funktionen verwendet *ServerView Suite* die Ports 8881 bis 8883, die in der Datei */opt/SMW/SMWapac/conf/http_addWSA.conf* konfiguriert sind. Diese Ports werden nur benötigt, wenn Web-Server-Funktionen wie Java Web Start, das Herunterladen von Anwendungen, usw. verwendet werden sollen.

Die Ports werden wie folgt eingesetzt:

- 8881: Java Web Start für Lese-Schreib-Zugriff
- 8882: Java Web Start für Nur-Lese-Zugriff
- 8883: Download-Seite für JRE, Windows-Anwendung, Online-Handbücher, Java Policy Template

8.1.2 Fest zugewiesene Ports auf den verwalteten Knoten

8.1.2.1 Windows-System: PRIMERGY- und PRIMEQUEST-Systeme

SNMP-Aufträge müssen über Port 161 empfangen werden. Die diesbezüglichen Standard-Systemeinstellungen sollten daher nicht verändert werden.

Port 3172 wird vom Agenten des Performance-Managers für die Kommunikation mit dem Management-Server verwendet

8.1.2.2 Linux-System

SNMP-Aufträge müssen über Port 161 empfangen werden. In `/etc/services` müssen daher folgende Zeilen eingetragen sein:

snmp	161/tcp	#Simple Net Mgmt Proto
snmp	161/udp	#Simple Net Mgmt Proto
dom_adm	8899/udp	#Port für Domänenverwaltungsservice

Tabelle 4: Zeilen, die für SNMP-Aufträge in der Datei `/etc/services` eingetragen werden müssen

Port 3172 wird vom Agenten des Performance-Managers belegt.

8.1.2.3 Solaris-Systeme

Bei der Installation des *ServerView Suite Agent* wird in der Datei `/etc/services` folgender Eintrag erstellt:

dom_adm	8899/udp	#Port für Domänenverwaltungsservice
---------	----------	-------------------------------------

Tabelle 5: Beim Start der *ServerView Suite* in der Datei `/etc/services` angelegter Eintrag Entry

Zusätzlich wird der Port 23460 für die SSH-Kommunikation verwendet.

8.1.2.4 MMB

Port 22 wird für die SSH-Kommunikation verwendet.

snmp	161/tcp	#Simple Net Mgmt Proto
snmp	161/udp	#Simple Net Mgmt Proto

Tabelle 6: Einträge in der Datei */etc/services* für die MMB-SSH-Kommunikation

8.1.2.5 XSCF

Port 22 wird für die SSH-Kommunikation verwendet.

8.1.3 Rekonfigurierung von Port 8886: WSAserver

Gehen Sie bei der Änderung des UPD-Ports für den WSAserver-Dienst sehr sorgfältig vor, da die Portnummer auf dem Management-Server und auf allen der Verwaltungsarbeitsplätzen geändert werden muss.

Änderung auf dem Management-Server:

1. Editieren Sie die Datei */etc/services* und starten Sie den verwendeten Intranet-Dämon (*inetd* oder *xinetd*) neu.
2. Ändern Sie die Dateien */opt/SMAS/public_html/wsa.jnlp* und *wsa_ro.jnlp*, falls Sie die *ServerView Suite* über den Browser als Java Web Start-Anwendung aufrufen möchten.

Änderung auf dem Verwaltungsarbeitsplatz:

- Linux-System:

Ändern Sie die Datei *opt/SMAS/bin/svsee* und fügen Sie die Option *-port <new_portnumber>* in die Java-Startzeile ein.

- Windows-System:

Ändern Sie die Datei *<installation_directory>\wsa.bat* und fügen Sie die Option *-port <new_portnumber>* in die Java-Startzeile ein.

8.1.4 Rekonfigurierung von Port 8899: dom_adm

Gehen Sie bei der Änderung des UPD-Ports für den *dom_adm*-Dienst sehr sorgfältig vor, da die Portnummer auf dem Management-Server und auf allen verwalteten Linux- und Solaris-Knoten geändert werden muss.

Änderung auf dem Management-Server:

- Ändern Sie die Datei */etc/services* und starten Sie den verwendeten Intranet-Dämon (*inetd* oder *xinetd*) neu.

Änderung auf allen verwalteten Linux- und Solaris-Knoten mit ServerView Suite-Agent:

- Ändern Sie die Datei */etc/services* und starten Sie den verwendeten Intranet-Dämon (*inetd* oder *xinetd*) neu.



Bei Verwendung einer Firewall sorgen Sie dafür, dass der *dom_adm*-Port in der Übertragungsrichtung vom Management-Server zum verwalteten Knoten transparent ist.

8.1.5 Rekonfigurierung der Ports 8881-8883: Webserver-Ports

ServerView Suite benutzt die Ports mit den Nummern 8881, 8882 und 8883:

- 8881: Java Web Start für Lese-Schreib-Zugriff
- 8882: Java Web Start für Nur-Lese-Zugriff
- 8883: Download-Seite für JRE, Windows-Anwendung, Online-Handbücher, Java Policy Template

Wenn diese Portnummern bereits von anderen Anwendungen benutzt werden, können für die *ServerView Suite* stattdessen Portnummern im Bereich 1024 bis 65536 benutzt werden. Gehen Sie dazu wie folgt vor:

- ▶ Melden Sie sich auf dem betreffenden Server als *root* an.
- ▶ Wechseln Sie in das Verzeichnis */opt/SMAW/public_html* und ändern Sie mittels eines Editors in den Dateien *wsa.jnlp*, *wsa_ro.jnlp*, *help.jnlp* und *help_ro.jnlp* die genannten Portnummern.

- ▶ Ändern Sie die Datei `/opt/SMAW/SMAWapac/conf/http_addWSA.conf` auf dem Management-Server:

Beispiel

Portnummer 8882 durch Portnummer 9992 ersetzen:

- Ändern Sie *Listen 8882* in *Listen 9992*
- Ändern Sie `<VirtualHost _default_:8882>` in `<VirtualHost _default_:9992>`

Starten Sie anschließend den WebServer neu:

- ▶ Red Hat: `/etc/init.d/httpd restart`
- ▶ SUSE: `/etc/init.d/apache2 restart`

8.2 Dynamisch zugewiesene Ports

Dynamisch zugewiesene Ports werden mithilfe von XML-Dateien festgelegt. Wie viele Ports benötigt werden, hängt von der Art der Verbindung sowie von der Anzahl Systeme ab, die angeschlossen werden sollen und muss sorgfältig berechnet werden. Details hierzu werden in den folgenden Kapiteln erläutert.

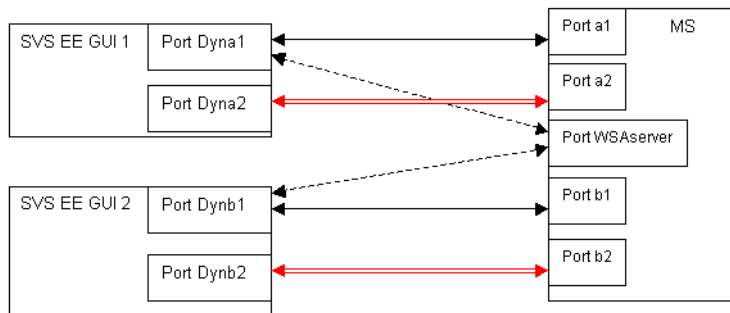
8.2.1 Dynamisch zugewiesene Ports auf dem Verwaltungsarbeitsplatz

Auf dem Verwaltungsarbeitsplatz wird für jede GUI-Instanz von *ServerView Suite* mindestens ein Port benötigt. Bei einer SSL-Kommunikation wird für jede GUI-Instanz zusätzlich ein weiterer Port benötigt.

Darüber hinaus öffnet die *ServerView Suite*-Anwendung für jeden Batch-Auftrag einen weiteren Port. Bei diesen Batch-Aufträgen handelt es sich um:

- PRIMEPOWER Enterprise Server Alignment
- Dynamic Reconfiguration

Die folgende Abbildung zeigt die Kommunikationspfade, die eingerichtet werden, wenn zwei *ServerView Suite*-Anwendungen auf einem Verwaltungsarbeitsplatz laufen und beide über SSL mit demselben Management-Server verbunden sind.



====> TCP/IP mit SSL

==> TCP/IP

-----> UDP

Bild 7: Kommunikationspfade

Die Konfiguration wird in der Datei *C:\wsa_certs\WSALocalPreferences.xml* festgelegt.

Wenn Sie den Bereich der zu verwendenden Ports ändern wollen, müssen Sie folgendermaßen vorgehen:

1. Erstellen Sie das Verzeichnis *C:\wsa_certs* (auf Windows) bzw. */opt/SMAW/wsa_certs* (auf Linux)
2. Rufen Sie die *ServerView Suite*-Anwendung auf und beenden Sie sie wieder. Dadurch wird die Konfigurationsdatei *WSALocalPreferences.xml* in dem obigen Verzeichnis angelegt.
3. Passen Sie die folgenden Attribute in der Konfigurationsdatei *WSALocalPreferences.xml* Ihren Erfordernissen an:

```
<void property="maxUDPport">
  <int>3100</int>
</void>
<void property="minUDPport">
  <int>3000</int>
</void>
```

8.2.2 Dynamisch zugewiesene Ports auf dem Management-Server

Die Port-Konfiguration wird in der Datei `/opt/SMAW/users/preferences.xml` festgelegt. Die Änderungen können mit Hilfe eines Editors vorgenommen werden.

1. Für jede gleichzeitig bestehende Verbindung zwischen Verwaltungsarbeitsplatz und dem Management-Server wird mindestens ein Port auf dem Managementserver benötigt. Bei einer SSL-Kommunikation werden für jede gleichzeitig bestehende Serververbindung zwei Ports benötigt. Darüber hinaus wird für jeden parallel laufenden Batch-Auftrag ein Server-Port benötigt.

Passen Sie die folgenden Attribute Ihren Erfordernissen an:

```
<!-- WSA Min Port -->
<WsaMinPort>10000</WsaMinPort>
<!-- WSA Max Port -->
<WsaMaxPort>65535</WsaMaxPort>
```

Diese Änderungen können auch über das SVS EE-GUI (*Edit* → *Preferences* → *General*) erfolgen.

2. Für jeden verwalteten Knoten, auf dem *ServerView Suite Agent* installiert ist, werden drei dynamisch zugewiesene Domänenports benötigt. Wenn also 50 Knoten durch den Management-Server verwaltet werden, müssen mindestens 150 Ports reserviert werden.

Passen Sie die folgenden Attribute Ihren Erfordernissen an:

```
<!-- Domain Min Port -->
<DomainMinPort>20000</DomainMinPort>
<!-- Domain Max Port -->
<DomainMaxPort>65535</DomainMaxPort>
```

Diese Werte müssen nur auf dem Management-Server geändert werden.



Beachten Sie, dass die Kommunikation vom verwalteten Knoten initiiert wird. Die oben konfigurierte Portnummer gilt für den Management-Server. Folglich muss die Firewall zwischen dem Management-Server und dem verwalteten Knoten für Port 8899 in der Übertragungsrichtung vom Management-Server zum verwalteten Knoten transparent sein. Die Ports im Konfigurationsbereich `DomainMinPort/DomainMaxPort` müssen für die Firewall in umgekehrter Übertragungsrichtung transparent sein.

Die folgende Abbildung zeigt die Kommunikationspfade zwischen dem Management-Server und den verwalteten Knoten während einer Sitzung:

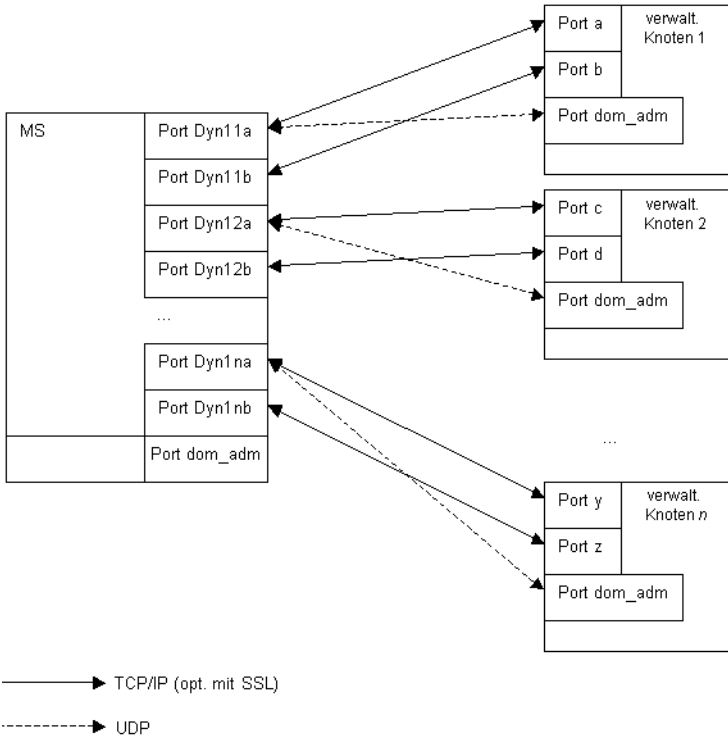


Bild 8: Kommunikationspfade

Wobei

```
dom_adm == 8899
DomainMinPort <= PortDyn1xx <= DomainMaxPort
1024 <= Port x <= 65535
```

8.2.3 Rekonfigurierung dynamisch zugewiesener Ports

Die Bereiche dynamisch zugewiesener Ports können problemlos rekonfiguriert werden. Editieren Sie dazu die genannten Konfigurationsdateien (siehe [Abschnitt „Dynamisch zugewiesene Ports auf dem Management-Server“ auf Seite 65](#)) auf dem Management-Server und starten Sie das GUI neu.

9 PRIMEQUEST konfigurieren

Das PRIMEQUEST-System und der *ServerView Suite* Management-Server müssen beide konfiguriert werden, bevor die PRIMEQUEST der Domäne auf dem Management-Server hinzugefügt wird.

9.1 Einstellungen im MMB-Web UI

Zur Konfiguration des PRIMEQUEST-Servers wird das *MMB Web-UI* verwendet. Näheres hierzu finden Sie in Kapitel „Setup“ des aktuellen *PRIMEQUEST Installation Manual* sowie in Part III „MMB“ des aktuellen *PRIMEQUEST Reference Manual: Basic Operation/GUI/Commands*.



Verwaltungs-LAN und Geschäfts-LAN müssen unterschiedlichen Teilnetzen angehören.

Näheres hierzu erfahren Sie im Abschnitt „LAN configuration (management LAN/private LAN/business LAN)“ des aktuellen *PRIMEQUEST Design Guide*.



PRIMEQUEST Server Agent (PSA) muss entsprechend konfiguriert sein.

Näheres hierzu finden Sie im Kapitel „Work Required After Operating System Installation“ des aktuellen *PRIMEQUEST Installation Manual*.

9.1.1 Verwaltungs-LAN konfigurieren

PRIMEQUEST-Server verfügen über einen integrierten Netzwerkschalter zur Schaltung des Verwaltungs-LANs, so dass verschiedene Modi eingestellt werden können. Konfigurieren Sie den PRIMEQUEST-Verwaltungsport wie folgt:

Rufen Sie im *MMB Web-UI* die Menüoptionen *Network Configuration* → *Management LAN Port Configuration* auf und aktivieren Sie

- *VLAN Mode* (Kommunikation zwischen den Partitionen wird zugelassen)
oder
- *No VLAN Mode* (Kommunikation zwischen den Partitionen ist nicht zugelassen).

Port Disable Mode darf nicht aktiviert werden, weil sonst keine Informationen über die Partitionen ermittelt werden können



Model: PRIMEQUEST 480

Part Number: MC5A0P111S

Serial Number: 6B03284266, 1030536001

Status: Normal

Active:MMB#0

System Partition Switch User Administration **Network Configuration** Maintenance

>Network Configuration >Management LAN Port Configuration

☐ Date/Time
☐ Network Interface
☒ Management LAN Port Config
☐ Network Protocols
☐ Refresh Rate
☐ SNMP Configuration
☐ SSL
☐ SSH
☐ Remote Server Management
☐ Access Control
☐ Alarm E-Mail
☐ License

Management LAN Port Configuration

Click the Apply Button to apply all changes.

VLAN Mode
☐ No VLAN Mode
☒ VLAN Mode
 The communication between partition(s) is disabled.
☐ Port Disable Mode
 The communication between partition(s) and between partition(s) and MMB's port(s) is disabled.

Speed/Duplex for MMB#0

User Port	Auto
Maintenance Port	Auto
REMCS Port	Auto

Speed/Duplex for MMB#1

User Port	Auto
Maintenance Port	Auto
REMCS Port	Auto

Apply Cancel

Bild 9: Verwaltungsport konfigurieren

Näheres hierzu finden Sie im Kapitel „Setup“ des aktuellen *PRIMEQUEST Installation Manual*.

9.1.2 SNMP aktivieren

Rufen Sie im *MMB Web-UI* die Menüoptionen *Network Configuration* → *Network Protocols* auf und aktivieren Sie SNMP Agent und SNMP Trap.

FUJITSU Model: PRIMEQUEST 480 Active:MMB#0
 Part Number: MCSA0P111
 Serial Number: 1010449001
 Status: Normal

System Partition Switch User Administration Network Configuration Maintenance Logout
 > Network Configuration > Network Protocols

Network Protocols Help

Click the Apply Button for all changes to take effect.

Web (HTTP/HTTPS)

HTTP	☒ Enable ☐ Disable
HTTP Port#[1024-65535]	8081
HTTPS	☒ Enable ☐ Disable
HTTPS Port#[432,1024-65535]	432
Timeout (sec)	600

Telnet

Telnet	☐ Enable ☒ Disable
Telnet Port#[23,1024-65535]	23
Timeout (sec)	600

SSH

SSH	☐ Enable ☒ Disable
SSH Port#[22,1024-65535]	22
Timeout (sec)	600

SNMP

SNMP Agent	☒ Enable ☐ Disable
Agent Port#[161,1024-65535]	161
SNMP Trap	☒ Enable ☐ Disable
Trap Port#[162,1024-65535]	162

Apply Cancel

Bild 10: SNMP aktivieren

Folgende Einstellungen müssen vorgenommen werden:

SNMP Agent

Aktivieren Sie das Optionsfeld *Enable*.

Agent Port#

Stellen Sie die Portnummer *161* ein.

SNMP-Trap

Aktivieren Sie das Optionsfeld *Enable*.

Trap Port#

Stellen Sie die Portnummer *162* ein.

9.1.3 SNMP konfigurieren

9.1.3.1 SNMP-Protokollparameter

Rufen Sie im *MMB Web-UI* die Menüoptionen *Network Configuration* → *SNMP Configuration* → *Community* auf und setzen Sie die Parameter gemäß der verwendeten SNMP Protokollversion v1 ein.

FUJITSU Model: PRIMEQUEST 480 Active:MMB#0
 Part Number: MC5A0P111
 Serial Number: 1010449001
 Status: Normal

System Partition Switch User Administration Network Configuration Maintenance Logout

>Network Configuration >SNMP Configuration >Community

SNMP Community

Click the Apply Button for all changes to take effect.

System Information

System Name:
 System Location:
 System Contact:

Note/System Name can be configured in System->System Information page.

Community

Community	IP Address/MASK	SNMP Version	Access	Auth
trunpl	10.124.17.79	1	Read Only	noauth
ssnwr	10.124.17.72	1	Read Only	noauth
		1	Read Only	noauth
		1	Read Only	noauth
		1	Read Only	noauth
		1	Read Only	noauth
		1	Read Only	noauth
		1	Read Only	noauth
		1	Read Only	noauth
		1	Read Only	noauth
		1	Read Only	noauth
		1	Read Only	noauth
		1	Read Only	noauth
		1	Read Only	noauth
		1	Read Only	noauth
		1	Read Only	noauth
		1	Read Only	noauth
		1	Read Only	noauth
		1	Read Only	noauth
		1	Read Only	noauth
		1	Read Only	noauth
		1	Read Only	noauth
		1	Read Only	noauth

Apply Cancel

Bild 11: SNMP-Protokollparameter

Folgende Einstellungen müssen vorgenommen werden:

Community

Geben Sie eine Community (max. 32 Zeichen, Standard: *public*) zur Kommunikation mit dem Management-Server ein.

IP Address/MASK

Geben Sie die IP-Adresse und die Netzwerkmaske des Management-Servers ein, der die PRIMEQUEST verwaltet.

SNMP Version

Setzen Sie die Protokollversion auf *1*.

Access

Wählen Sie die Zugriffsberechtigung *Read Write*.

Auth

Geben Sie *noauth* an.

9.1.3.2 SNMP-Trap-Parameter

Rufen Sie im *MMB Web-UI* die Menüoptionen *Network Configuration* → *SNMP Configuration* → *Trap* auf und setzen Sie die Parameter gemäß der verwendeten SNMP Protokollversion v1.

Model: PRIMEQUEST 480
Part Number: MCSA0P111
Serial Number: 1010449001
Status: Normal

System Partition Switch User Administration Network Configuration Maintenance Logout

> Network Configuration > SNMP Configuration > Trap

SNMP Trap

Click the Apply Button for all changes to take effect.

Trap Destination

Community/User	IP Address	SNMP Version	Auth	Auth Type	Auth passphrase Priv passphrase
☐ public	10 . 24 . 17 . 29	1	noauth	MD5	
☐	0 . 0 . 0 . 0	1	noauth	MD5	
☐	0 . 0 . 0 . 0	1	noauth	MD5	
☐	0 . 0 . 0 . 0	1	noauth	MD5	
☐	0 . 0 . 0 . 0	1	noauth	MD5	
☐	0 . 0 . 0 . 0	1	noauth	MD5	
☐	0 . 0 . 0 . 0	1	noauth	MD5	
☐	0 . 0 . 0 . 0	1	noauth	MD5	
☐	0 . 0 . 0 . 0	1	noauth	MD5	
☐	0 . 0 . 0 . 0	1	noauth	MD5	
☐	0 . 0 . 0 . 0	1	noauth	MD5	
☐	0 . 0 . 0 . 0	1	noauth	MD5	
☐	0 . 0 . 0 . 0	1	noauth	MD5	
☐	0 . 0 . 0 . 0	1	noauth	MD5	
☐	0 . 0 . 0 . 0	1	noauth	MD5	

Apply Cancel Test Trap

Bild 12: SNMP-Trap

Folgende Einstellungen müssen vorgenommen werden:

Community/User

Geben Sie hier *public* ein.

IP Address

Geben Sie die IP-Adresse des SVS EE-Management-Servers an.

SNMP Version

Wählen Sie *SNMP version 1*.

Auth

Machen Sie hier keine Angabe.

Auth Type

Machen Sie hier keine Angabe.

Auth passphrase/Priv passphrase

Machen Sie hier keine Angabe.

9.1.4 Access Control konfigurieren

Der MMB muss so konfiguriert werden, dass der Management-Server für die Protokolle SNMP Zugriffsrechte erhält.

Rufen Sie hierzu im *MMB Web-UI* die Menüoptionen *Network Configuration* → *Access Control* auf.

Ist kein Filter für das Protokoll SNMP eingestellt, so ist der Zugriff nicht beschränkt, d. h. Sie brauchen keinen Filter zu konfigurieren.

Existiert ein Filter, so muss der Zugriff vom Management-Server ebenfalls explizit über einen Filter erlaubt werden. Sie erzeugen einen neuen Filter, indem Sie die *Add*-Schaltfläche betätigen und in dem angezeigten Menu auswählen:

- *Protocol*: SNMP
- *Access Control*: wählen Sie *Enable*
- *IP Address*: IP-Adresse des Management-Servers
- *Subnet Mask*: Netzwerkbereich, von dem aus der Zugriff erlaubt ist. Geben Sie 255.255.255.255 an, falls nur der Zugriff vom Management-Server unter *IP Address* erlaubt ist.

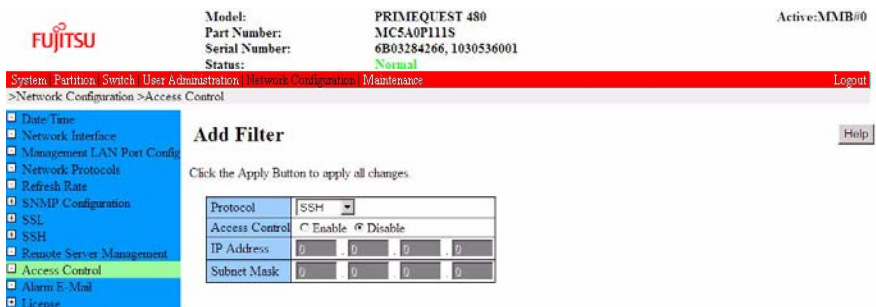


Bild 13: Filter anlegen

9.1.5 Remote Server Management konfigurieren

Folgende Einstellungen müssen vorgenommen werden:

Rufen Sie im *MMB Web-UI* die Menüoptionen *Network Configuration* → *Remote Server Management* auf und stellen Sie die Parameter wie folgt ein.



Bild 14: Remote Server Management

User Name

Markieren Sie den Benutzernamen. Wählen Sie einen Benutzer mit Systemverwalterrechten.

Markieren Sie den entsprechenden *User Name* und klicken Sie dann auf die Schaltfläche *Edit*. Es erscheint das folgende Fenster:

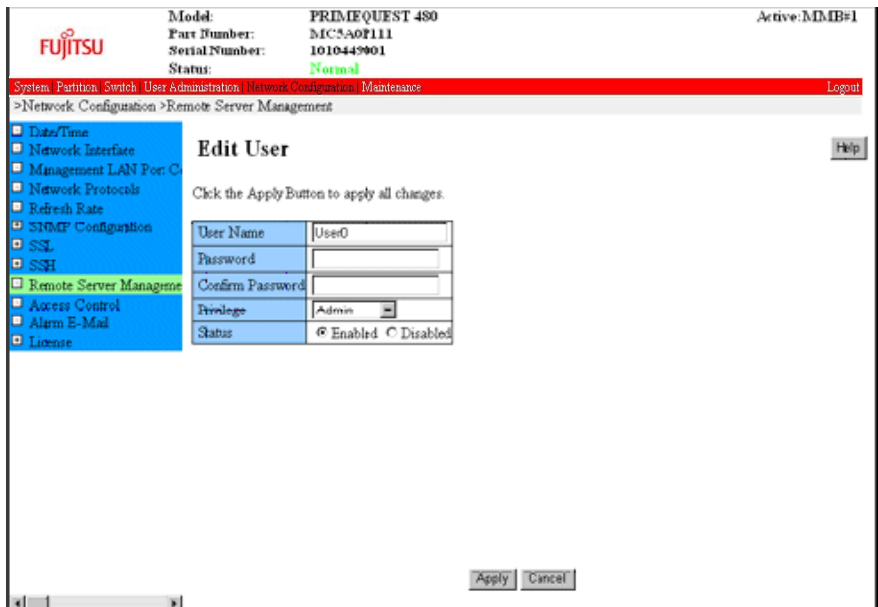


Bild 15: Remote Server Management: Edit User

User Name/Password/Confirm Password

Geben Sie Benutzerkennung und Passwort für die Kommunikation mit dem management-Server ein.

Privilege

Wählen Sie *Admin* aus dem Listenfeld.

Status

Aktivieren Sie den ausgewählten Benutzer.

9.2 IP-Adresse des MMB ändern

Wenn Sie die IP-Adresse des PRIMEQUEST *Management Board (MMB)* ändern, muss auch die Definition des Management-Servers entsprechend aktualisiert werden.

Ändern Sie die IP-Adresse des MMB wie folgt:

- ▶ Entfernen Sie den PRIMEQUEST-Server, dessen Adresse geändert werden soll, mittels des SVS EE-GUI aus der Domäne.
- ▶ Ändern Sie die IP-Adresse des MMB mit Hilfe des *MMB Web-UI*.
- ▶ Rufen Sie die *ServerView Suite* auf und fügen Sie den PRIMEQUEST-Server wieder zur Domäne hinzu.

9.3 Konfiguration der Partition ändern

Wenn Sie mit dem *MMB Web-UI* die Partitionskonfiguration eines PRIME-QUEST-Servers ändern, wird automatisch die Definition des Management-Servers aktualisiert, falls Partitionen angelegt oder gelöscht werden.

Falls Linux-Partitionen in einer der Applikationen (*Config/User/Process/Task* etc.) ausgegraut bleiben:

- ▶ Überprüfen Sie, ob PSA (PRIMEQUEST Server Agent) in der Partition korrekt installiert ist.
- ▶ Rufen Sie die *Domain*-Applikation auf und aktualisieren Sie die Oberfläche über die *Refresh all*-Schaltfläche.

9.4 Aktualisieren von Management-Server-Einstellungen

Wenn auf einem verwalteten PRIMEQUEST-Server Änderungen an der SNMP-Konfiguration (siehe [Abschnitt „SNMP konfigurieren“ auf Seite 73](#)) oder der Konfiguration von *Remote Server Management* (siehe [Abschnitt „Remote Server Management konfigurieren“ auf Seite 78](#)) vorgenommen wurden, müssen anschließend in gleicher Weise die Einstellungen auf dem Management Server aktualisiert werden.

Gehen Sie hierzu wie folgt vor:

- ▶ Wählen Sie in der Applikation *Domain* in der Objekt-Tabelle das MMB des Zielsystems aus.
- ▶ Klicken Sie mit der rechten Maustaste auf das MMB und wählen Sie im Kontextmenü *Modify*.
- ▶ Ändern Sie in der Dialog-Box die Einstellung für den PRIMEQUEST-Server.

10 SPARC ES konfigurieren

Der SPARC Enterprise Server und der Management-Server der *ServerView Suite Enterprise Edition* müssen eingerichtet sein, bevor der SPARC Enterprise Server der Domäne auf dem Management-Server hinzugefügt wird.

Die *ServerView Suite Enterprise Edition* benutzt SSH zur Verwaltung von SPARC Enterprise Servern. Entsprechend den folgenden zwei Abschnitten müssen die SSH-Schlüssel mit dem Management-Server ausgetauscht werden, bevor der Server der Domäne hinzugefügt wird.

10.1 Öffentlicher SSH-Schlüssel des XSCF-Boards

Der öffentliche SSH-Schlüssel muss auf dem Management-Server und dem XSCF-Board installiert werden. Gehen Sie hierbei wie im Folgenden beschrieben vor.



Die in diesem Abschnitt beschriebenen Prozeduren sind für einige Modelle der SPARC Enterprise Server, die kein XSCF-Board haben (z.B. die T-Series-Modelle), nicht nötig.



Nähere Informationen zum XSCF-Board und seinen SSH-Einstellungen entnehmen Sie bitte dem *SPARC Enterprise Server M4000/M5000/M8000/M9000 Servers eXtended System Control Facility (XSCF) User's Guide*.

Überprüfen Sie folgende Anforderungen für das XSCF-Board:

- SSH ist eingeschaltet. Überprüfen Sie dies mit Hilfe des Kommandos *showssh*.
- Für die Kommunikation mit dem Management-Server muss ein Benutzerkonto mit den Privilegien *platadm* und *fieldeng* eingerichtet sein. Dieses Benutzerkonto wird dazu benutzt, den öffentlichen SSH-Schlüssel des Management-Servers auf dem XSCF-Board zu registrieren.

Öffentlichen SSH-Schlüssel des Management-Servers auf dem XSCF-Board registrieren

- ▶ Melden Sie sich auf dem Management-Server als *root* an.
- ▶ Führen Sie das folgende Kommando aus, um den öffentlichen SSH-Schlüssel des Management-Servers anzuzeigen.

```
# /opt/FJSVap1sc/sbin/ap1sc_ssh_pubkeyshow
```

- ▶ Melden Sie sich beim XSCF-Board über ein Benutzerkonto mit dem Privileg *useradm* an.
- ▶ Führen Sie das folgende Kommando auf dem XSCF-Board aus. Das Benutzerkonto mit den Privilegien *platadm* und *fieleng* muss als Argument der Option *-u* angegeben werden. Im folgenden Beispiel ist *platxscf* das Benutzerkonto.

```
XSCF> setssh -c addpubkey -u platxscf
```

Diese Kommando fordert den Benutzer auf, den SSH-Schlüssel einzugeben. Kopieren Sie den oben spezifizierten SSH-Schlüssel und fügen Sie ihn auf der XSCF-Konsole als Eingabe ein.

Starten Sie die Ausführung, indem Sie zuerst die Enter-Taste und danach Ctrl+D (EOF) drücken.

- ▶ Führen Sie das folgende Kommando aus, um zu prüfen, ob der öffentliche Schlüssel korrekt registriert ist.

```
XSCF> showssh -c pubkey -u platxscf
```

Öffentlichen SSH-Schlüssels des XSCF-Boards auf dem Management-Server registrieren



Die folgende Prozedur setzt voraus, dass das XSCF-Board und der Management-Server über ein sicheres Netzwerk verbunden sind.

Im folgenden Beispiel ist 192.168.20.10 die IP-Adresse des XSCF-Boards.

- ▶ Melden Sie sich auf dem Management-Server als *root* an.
- ▶ Führen Sie das folgende Kommando aus, um den öffentlichen SSH-Schlüssel des XSCF-Boards zu übernehmen. Das Benutzerkonto mit den Privilegien *platadm* und *fieleng* muss als Argument der Option *-u* angegeben werden. Im folgenden Beispiel ist *platxscf* das Benutzerkonto.

```
# /opt/FJSVap1sc/sbin/ap1sc_connect -scf -i 192.168.20.10 -u platxscf
```

10.2 Öffentlicher SSH-Schlüssel auf dem verwalteten Knoten

Der öffentliche SSH-Schlüssel muss auf allen verwalteten Knoten (Partitionen oder T-Series-Modelle) installiert werden. Gehen Sie hierbei wie im Folgenden beschrieben vor.



Die folgende Prozedur setzt voraus, dass der verwaltete Knoten und der Management-Server über ein sicheres Netzwerk verbunden sind.

Im folgenden Beispiel ist 192.168.20.20 die IP-Adresse des Agenten.

- Melden Sie sich auf dem Management-Server als *root* an.
- Führen Sie folgendes Kommando aus, um die öffentlichen SSH-Schlüssel des Management-Servers und der Partition auszutauschen.

```
# /opt/FJSVap1sc/sbin/ap1sc_connect -par -i 192.168.20.20
```



Wenn ein Passwort verlangt wird, geben Sie das Root-Passwort des verwalteten Knotens ein. Das Passwort kann bis zu dreimal angefordert werden.

10.3 Konfigurationsänderungen

In einigen Fällen kann es notwendig werden, die SSH-Konfiguration für das SPARC Enterprise System insgesamt oder für einzelne seiner Komponenten zu ändern. So kann z. B. eine Partition bereits eine Registrierung eines anderen Management-Servers haben.

In den folgenden Abschnitten wird beschrieben, welche Schritte jeweils zu unternehmen sind, um eine existierende SSH-Konfiguration zu ändern.

Im [Abschnitt „Agent mit bereits registrierter SSH-Information“ auf Seite 90](#) wird beschrieben, was zu tun ist, wenn die SSH-Information eines Agenten bereits vor dessen Installation beim Management-Server registriert ist.

10.3.1 Öffentlichen SSH-Schlüssel auf dem Management-Server ändern

Im folgenden Beispiel ist 192.168.20.10 die IP-Adresse des XSCF-Boards und 192.168.20.20 die des verwalteten Knotens.

- ▶ Melden Sie sich auf dem Management-Server als *root* an.
- ▶ Führen Sie die folgenden Kommandos aus, um die SSH-Information für das XSCF-Board und alle SPARC Enterprise-Server-Agenten zu löschen.

a) Für das XSCF-Board

```
# /opt/FJSVap1sc/sbin/ap1sc_disconnect -scf -i 192.168.20.10
```

b) Für den verwalteten Knoten

```
# /opt/FJSVap1sc/sbin/ap1sc_disconnect -par -i 192.168.20.20
```



Wenn ein Passwort verlangt wird, geben Sie das Root-Passwort des verwalteten Knotens ein.

- ▶ Führen Sie das folgende Kommando aus, um einen neuen öffentlichen Schlüssel für den Management-Server anzulegen.

```
# /opt/FJSVap1sc/sbin/ap1sc_ssh_keyreplace
```

- ▶ Führen Sie folgende Kommandos aus, um die SSH-Information für das XSCF-Board und alle Agenten des SPARC Enterprise Servers zu registrieren. Das Benutzerkonto mit den Privilegien *platadm* und *fieldeng* muss als Argument der Option *-u* angegeben werden. Im folgenden Beispiel ist *platxscf* das Benutzerkonto.

a) Für das XSCF-Board

```
# /opt/FJSVap1sc/sbin/ap1sc_connect -scf -i 192.168.20.10 -u platxscf
```

b) Für den verwalteten Knoten

```
# /opt/FJSVap1sc/sbin/ap1sc_connect -par -i 192.168.20.20
```



Wenn ein Passwort verlangt wird, geben Sie das Root-Passwort des verwalteten Knotens ein. Das Passwort kann bis zu dreimal angefordert werden.



Abhängig vom Zeitintervall kann der Status des verwalteten SPARC Enterprise Servers kurzfristig unbekannt sein, nachdem die SSH-Information gelöscht ist.

10.3.2 Öffentlichen SSH-Schlüssel oder IP-Adresse des XSCF-Boards ändern

- Löschen Sie den SPARC Enterprise Server aus der Domäne in der *ServerView Suite Enterprise Edition*.
- Melden Sie sich auf dem Management-Server als *root* an.
- Führen Sie das folgende Kommando aus, um die SSH-Information für das XSCF-Board zu löschen.

```
# /opt/FJSVap1sc/sbin/ap1sc_disconnect -scf -i 192.168.20.10
```

- Ändern Sie die XSCF-Betriebsumgebung.



Einzelheiten zur Änderung der XSCF-Betriebsumgebung entnehmen Sie bitte dem *SPARC Enterprise Server M4000/M5000/M8000/M9000 Servers eXtended System Control Facility (XSCF) User's Guide*.

- Führen Sie das folgende Kommando aus, um den öffentlichen SSH-Schlüssel des XSCF-Boards zu akzeptieren. Das Benutzerkonto mit den Privilegien *platadm* und *fieldeng* muss als Argument der Option *-u* angegeben werden. Im folgenden Beispiel ist *platxscf* das Benutzerkonto.

```
# /opt/FJSVap1sc/sbin/ap1sc_connect -scf -i 192.168.20.10 -u platxscf
```

- Fügen Sie den SPARC Enterprise Server mit dem SVS EE GUI der Domäne hinzu.

10.3.3 Öffentlichen SSH-Schlüssel, Hostname oder IP-Adresse des verwalteten Knotens ändern

SSH-Schlüssel ändern

Verwenden Sie die folgende Prozedur, um den öffentlichen SSH-Schlüssel des verwalteten Knotens zu ändern.

- Melden Sie sich auf dem Management-Server als *root* an.
- Führen Sie folgendes Kommando aus, um die SSH-Information für den SPARC Enterprise Server-Agenten zu löschen.

```
# /opt/FJSVap1sc/sbin/ap1sc_disconnect -par -i 192.168.20.20
```



Wenn ein Passwort verlangt wird, geben Sie das Root-Passwort des verwalteten Knotens ein.



Falls der Hostname oder die IP-Adresse vor dem Löschen des Agenten geändert wurde, erfolgt eine Warnung, die ignoriert werden kann.

- Melden Sie sich auf dem verwalteten Knoten als *root* an.

- Stoppen Sie den SPARC Enterprise Server-Agenten.

```
# /opt/FJSVaplsa/sbin/svsagtctl stop
```

- Führen Sie folgendes Kommando aus, um einen neuen öffentlichen Schlüssel für den verwalteten Knoten anzulegen.

```
# /opt/FJSVaplsa/sbin/svsagt_ssh_keyinit
```

- Starten Sie den SPARC Enterprise Server-Agenten erneut.

```
# /opt/FJSVaplsa/sbin/svsagtctl start
```

- Führen Sie das folgende Kommando auf dem verwalteten Server aus, um den öffentlichen SSH-Schlüssel des verwalteten Servers und der Partition auszutauschen.

```
# /opt/FJSVap1sc/sbin/ap1sc_connect -par -i 192.168.20.20
```



Wenn ein Passwort verlangt wird, geben Sie das Root-Passwort des verwalteten Knotens ein. Ein Passwort kann bis zu dreimal angefordert werden.

Hostname oder IP-Adresse ändern

Verwenden Sie die folgende Prozedur, um den Hostnamen oder die IP-Adresse des verwalteten Knotens zu ändern.

- Löschen Sie den SPARC Enterprise Server mit dem SVS EE GUI aus der Domäne, dessen Hostname oder IP-Adresse geändert wurde.
- Melden Sie sich auf dem verwalteten Knoten als *root* an.
- Ändern Sie den Hostnamen oder die IP-Adresse des verwalteten Knotens
- Ändern Sie den öffentlichen Schlüssel entsprechend der oben beschriebenen Prozedur.
- Fügen Sie den SPARC Enterprise Server mit dem SVS EE GUI der Domäne hinzu.

10.3.4 Portnummer für die SSH-Kommunikation ändern

Die *ServerView Suite Enterprise Edition* benutzt standardmäßig die Portnummer 23460 für die SSH-Kommunikation.

Dies ist ein Beispiel, wie die Portnummer auf 23400 geändert werden kann.

- Melden Sie sich auf dem Management-Server als *root* an.
- Löschen Sie den SPARC Enterprise Server mit dem SVS EE GUI aus der Domäne

```
# /opt/FJSVap1sc/sbin/ap1sc_disconnect -par -i 192.168.20.20
```



Wenn ein Passwort verlangt wird, geben Sie das Root-Passwort des verwalteten Knotens ein.

- Melden Sie sich auf dem verwalteten Knoten als *root* an.
- Fügen Sie den folgenden Porteintrag in die Datei */etc/inet/services* im richtigen Format ein. Falls dieser Eintrag schon vorhanden ist, prüfen Sie, ob die Portnummer korrekt ist.

```
rcxsshport 23400/tcp
```

- Starten Sie den SPARC Enterprise Server Agenten erneut.

```
# /opt/FJSVap1sa/sbin/svsagtctl stop
```

```
# /opt/FJSVap1sa/sbin/svsagtctl start
```

- Melden Sie sich auf dem Management-Server als *root* an.
- Führen Sie folgendes Kommando aus, um den SPARC Enterprise Server Agenten auszutauschen.

```
# /opt/FJSVap1sc/sbin/ap1sc_connect -par -i 192.168.20.20 -p 23400
```



Wenn ein Passwort verlangt wird, geben Sie das Root-Passwort des verwalteten Knotens ein. Das Passwort kann bis zu dreimal angefordert werden.

10.3.5 Agent mit bereits registrierter SSH-Information

Falls ein Agent, dessen SSH-Information bereits auf dem Management-Server registriert ist, auf dem Server installiert ist, müssen Sie zuerst die SSH-Information vom Management-Server löschen.

- Melden Sie sich auf dem Management-Server als *root* an.
- Führen Sie das folgende Kommando aus, um zu prüfen, ob die SSH-Information für den Agenten auf dem Management-Server registriert ist.

```
# /opt/FJSVap1sc/sbin/ap1sc_ssh_registered -i 192.168.20.20
```

Falls ein Text wie der Folgende angezeigt wird, ist die SSH-Information bereits registriert.

```
192.168.20.20 23460
```

- Falls die SSH-Information bereits registriert ist, löschen Sie sie vom Management-Server.

```
# /opt/FJSVap1sc/sbin/ap1sc_disconnect -par -i 192.168.20.20
```



Wenn ein Passwort verlangt wird, geben Sie das Root-Passwort des verwalteten Knotens ein. Die folgende Warnung wird angezeigt, kann aber ignoriert werden:

```
can't delete remote user public key
```

11 Anhang

11.1 Konfiguration der SV-SNMP-Agenten unter Linux

Die Konfigurationsdatei für die ServerView-Agenten ist `/etc/srvmagt/config`.

Zeilen, die mit # beginnen, sind Kommentarzeilen. Andere Zeilen haben das Format:

`<schlüsselwort>=<wert>`

- *AgentPermission*

Prinzipielle Erlaubnis für andere Systeme, Werte auf dem lokalen Knoten mit Hilfe von SNMP-Kommandos zu setzen (2: nicht erlaubt, 3: erlaubt, Voreinstellung: 2).

Falls Sie diese SNMP-Set-Requests zulassen wollen, müssen Sie hier den Wert auf „3“ setzen sowie die SNMP-Dienste entsprechend konfigurieren (siehe hierzu [Kapitel „SNMP-Konfiguration“ auf Seite 39](#)).

- *AgentShut*

Erlaubnis für andere Systeme, einen Shutdown/Reboot auf dem lokalen Knoten mit SNMP-Kommandos durchzuführen (2: nicht erlaubt, 3: erlaubt, Voreinstellung: 2).

Falls Sie diese SNMP-Set-Requests zulassen wollen, müssen Sie hier den Wert auf „3“ setzen sowie die SNMP-Dienste entsprechend konfigurieren (siehe hierzu [Kapitel „SNMP-Konfiguration“ auf Seite 39](#)).

- *NoAccountCheck*

Wird hierfür ein anderer Wert als 0 festgelegt, so wird kein Passwort abgefragt, wenn über ServerView Einstellungen verändert werden. Die Standardeinstellung ist 0, d. h. standardmäßig ist die Benuterauthentifizierung eingeschaltet. In diesem Fall muss unter *UserGroup* eine Benutzergruppe angegeben sein, der der Benutzer angehören muss, der SET-Operationen durchführen können soll.

Beachten Sie, dass eine deaktivierte Passwortabfrage ein erhebliches Sicherheitsrisiko darstellen kann.

- *UserGroup*

Falls bei *NoAccountCheck* 0 angegeben wurde, benötigt ServerView am Management-Server eine Benutzer/Passwort-Kombination, um SNMP-Einstellungen verändern zu können. Der Benutzer muss, um Zugriffsberechtigung zu erhalten, derjenigen Gruppe angehören, die unter *UserGroup* festgelegt ist. Die Standardeinstellung ist *bin*, zu der auch *root* gehört.

Falls die hier angegebene Benutzergruppe noch nicht existiert, so muss sie nachträglich noch mit betriebssystemspezifischen Mitteln angelegt werden.

- *ShutdownDelay*

Legt die Zeitspanne (in Minuten) zwischen einem SNMP-Shutdown-Request und dem Shutdown fest.

- *ExpectMylex*

Wird hierfür ein anderer Wert als 0 festgelegt, so wird immer dann ein Trap veranlasst, wenn kein Mylex-GAM-Treiber vorhanden ist.

- *ScanTapeDevices*

Wird hierfür ein anderer Wert als 0 festgelegt, werden die Gerätedateien */dev/nst** für Magnetbandlaufwerke geöffnet, um deren aktuellen Status zu ermitteln. Diese Öffnung kann (abhängig vom Treiber) einen unbeabsichtigten Wechsel der Lese-/Schreibposition des Bandes auslösen. Falls das Band von mehreren Servern zugleich verwendet wird, stellt dieser Parameter sicher, dass ServerView laufende Bandoperationen (z. B. Datensicherung) nicht durch Zustandsabfragen stört.

Die Standardeinstellung ist 0, d.h. Bandgerätedateien werden nicht geöffnet.



Eine Änderung der Datei *config* wird erst nach einem Neustart des Agenten wirksam. Dazu starten Sie den verwalteten Knoten neu oder geben folgendes Kommando als Systemverwalter ein:

```
# /etc/init.d/srvmagt restart
```

11.2 Konfiguration der SV-SNMP-Agenten unter Windows

Sie können die Konfiguration der ServerView-SNMP-Agenten ändern, indem Sie *Start* → *All Programs* → *Fujitsu* → *ServerView* → *Agents* → *Configuration* anwählen. Es wird ein Fenster mit folgenden drei Registerkarten geöffnet:

- *Trap Forwarding*
- *System Shutdown*
- *Security Settings*

Registerkarte „Trap Forwarding“

Alle SNMP-Traps, die von den ServerView-Agenten erzeugt werden, können optional in die System-Ereignisanzeige oder als Administrator-Meldung weitergeleitet werden. Die Weiterleitung hängt von der Gewichtung des Traps ab. Es gibt folgende Gewichtungsstufen:

- critical (kritische Traps)
- major (wichtige Traps)
- minor (weniger wichtige Traps)
- informational (informative Traps)

Die Abbildung der Gewichtung auf den Typ der Ereignisanzeige erfolgt folgendermaßen:

Trap-Gewichtung	Typ in der Ereignisanzeige
Critical and major traps	Fehler
Minor traps	Warnung
Informational traps	Information

Tabelle 7: Gewichtung der Ereignisanzeige-Typen

Für eine Weiterleitung der Traps an den Administrator muss der Nachrichtendienst auf dem Server konfiguriert und gestartet sein. Außerdem müssen die Ziele für die Meldungen in den Eigenschaften des Windows Server Manager konfiguriert werden.

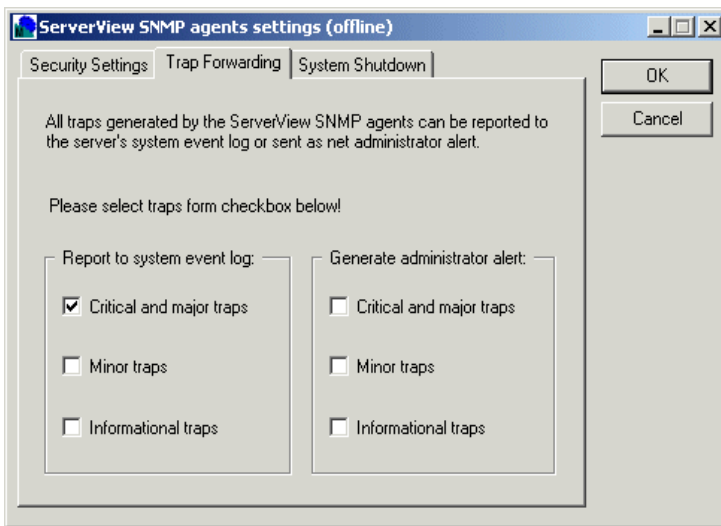


Bild 16: Registerkarte „Trap Forwarding“

Sie können auf der Registerkarte *Trap Forwarding* auswählen, welche SNMP-Traps wohin weitergeleitet werden sollen. Standardmäßig werden die kritischen und die wichtigen Traps an den SVS EE-Manager weitergeleitet.

Registerkarte „System Shutdown“

Die ServerView-Agenten können einen System-Shutdown initiieren. Die Aktivierung dieser Funktion wird jedoch nicht durch SVS EE unterstützt.

Registerkarte „Security Settings“

Die ServerView SNMP-Agenten bieten in Verbindung mit dem Management-Server ein erweitertes Sicherheitskonzept, um SNMP-SET-Operationen auf dem Server einzuschränken. Es besteht die Möglichkeit, SET-Operationen generell zu verbieten oder in Verbindung mit dem Management-Server durch eine Benutzer-Authentifizierung zu schützen.

Ist die Benutzer-Authentifizierung aktiviert, so wird vor jeder Ausführung einer SET-Operation eine Benutzer-Authentifizierung durchgeführt. Verläuft diese erfolgreich, so wird zusätzlich die Zugehörigkeit zu einer vom Administrator vergebenen Benutzergruppe überprüft.



Die Benutzer-Authentifizierung funktioniert nur mit ServerView auf dem Management-Server und ist für andere SNMP-Tools wirkungslos.

Sie können die Konfiguration der Sicherheitseinstellungen auf der folgenden Registerkarte vornehmen:

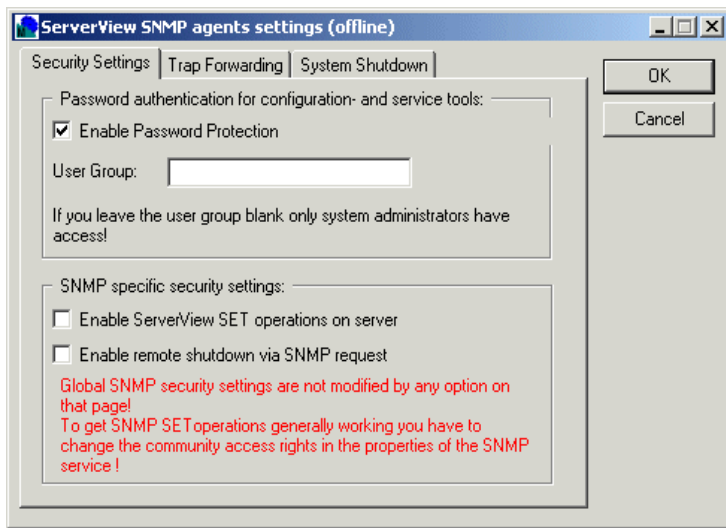


Bild 17: Registerkarte „Security Settings“

Enable ServerView SET operations on server

Erlaubt SNMP-SET-Operationen für die ServerView-Agenten. Verboten Sie SET-Operationen, so werden alle SNMP-SETs generell abgewiesen, unabhängig davon, mit welchem Tool der SET durchgeführt wird.



Diese Option gilt nur für ServerView-Agenten. Set-Operationen für andere SNMP-Agenten werden davon nicht beeinflusst.

Enable Password Protection

Schaltet die Benutzer-Authentifizierung für SNMP-SET-Operationen ein bzw. aus.

User Group

Gibt die Benutzergruppe an, zu der die Benutzer gehören müssen, die SET-Operationen auf dem Server ausführen dürfen. Sie können hier eine beliebige Benutzergruppe anlegen.

Falls die Benutzergruppe noch nicht existiert, so müssen Sie die Benutzergruppe auf dem Server mit betriebssystemspezifischen Mitteln nachträglich noch anlegen.

An dieser Stelle wird aber der Benutzergruppe kein Benutzer zugeordnet. Die Zuordnung erfolgt vor oder auch nach der Installation der Agenten auf Betriebssystemebene. Aus Sicherheitsgründen ist es sinnvoll, nur einen Benutzer einzutragen.

Geben Sie für *User Group* keinen Namen an, so dürfen nur lokale System-Administratoren SET-Operationen auf dem Server ausführen.

Enable remote shutdown via SNMP request

Einige SET-Operationen bewirken einen Shutdown oder Neustart des Systems. Hier können Sie diese speziellen SET-Operationen zulassen oder verbieten.



Von den SVS EE-Komponenten werden keine Shutdown-/Neustart-Operationen veranlasst.

Abkürzungen

CLI

Command Line Interface - Kommandozeilenschnittstelle

ES

Enterprise Server

GUI

Graphical User Interface - graphische Benutzeroberfläche

ID

Identifizier - Identifikation

IP

Internetprotokoll

JRE

Java Runtime Environment

LAN

Local Area Network

MMB

Management Board

MS

Management-Sever

NFS

Network File System

PQ

PRIMEQUEST

PSA

PRIMEQUEST Server Agent

PW

PRIMEPOWER

Abkürzungen

PY

PRIMERGY

RHEL

Red Hat Enterprise Linux

SLES

SUSE Linux Enterprise Server

SNMP

Simple Network Management Protocol

SV

ServerView

SVS EE

ServerView Suite Enterprise Edition

TCP/IP

Transmission Control Protocol/Internet Protocol

UI

User Interface

URL

Uniform Resource Locator

VLAN

Virtual Local Area Network

WSA

Web-based System Administration

XVGA

eXtended Video Graphics Array

XSCF

eXtended System Control Facility

Stichwörter

A

Agenten

Konfiguration 38

Aufbau

selbstsigniertes

Benutzerzertifikat 51

sichere Domäne 50

D

Deinstallation

Management-Server 16

verwaltete Knoten 37

dynamisch zugewiesene Ports

Konfiguration 63

E

entfernter Server

PRIMEQUEST 78

F

fest zugewiesene Ports

Konfiguration 59

H

HTTP-Kommunikation 57

I

Installation

Management-Server 16

öffentliche und private

Schlüssel 53

verwaltete Knoten 32

Verwaltungsarbeitsplatz 25

K

Konfiguration

Agenten 38

SNMP 40, 41

Konfiguration der Partition

PRIMEQUEST 80

L

Life Cycle Modules 27

Life-Cycle-Module 33

M

Management-Server

Deinstallation 16

Installation 16

Konfiguration 40

Voraussetzungen 13

MMB

PRIMEQUEST 80

O

öffentliche und private Schlüssel

Installation 53

P

Portkonfiguration

dynamisch zugewiesene

Ports 63

fest zugewiesene Ports 59

PRIMEQUEST

entfernter Server 78

Konfiguration der Partition 80

MMB 80

SNMP-Protokollparameter 73

SNMP-Trap 71, 75

R

Registerkarte

SNMP Security Settings 94

System Shutdown 94

Trap Forwarding 93

S

Secure Sockets Layer (SSL) 49

selbstsigniertes Benutzerzertifikat

Aufbau 51

sichere Domäne

Aufbau 50

SNMP [38](#), [40](#), [41](#)

SNMP Security Settings [94](#)

SNMP-Protokollparameter

PRIMEQUEST [73](#)

SNMP-Trap

PRIMEQUEST [71](#), [75](#)

SSL (Secure Sockets Layer) [49](#)

System Shutdown [94](#)

T

Trap Forwarding [93](#)

V

verwaltete Knoten

Deinstallation [37](#)

Installation [32](#)

Konfiguration [41](#)

Voraussetzungen [29](#)

Verwaltungsarbeitsplatz

Installation [25](#)

Voraussetzungen [24](#)

Voraussetzungen

Management-Server [13](#)

verwaltete Knoten [29](#)

Verwaltungsarbeitsplatz [24](#)